HS SEDI
Homeland Security Systems Engineering and Development Institute

Spillage and Cloud Computing

Presented to the Information Security and Privacy Advisory Board (ISPAB)

A Review in Collaboration with the

Federal Chief Information Council (FCIOC)

Information Security and Identity Management Committee (ISIMC)

Network and Infrastructure Security Sub Committee (NISSC)

February 14, 2013

Homeland Security

Purpose

- **As the U.S. Government moves to use cloud computing, traditional methods for addressing the spillage of information may not be applicable in cloud computing**
- **The purpose of this briefing is provide a framework for the Chief Information Security Officers to develop policy and guidance for addressing spills in the cloud**
- **This briefing accomplishes this goal by**
  - Reviewing existing policy and guidance
  - Summarizing the issues from a literature review
  - Defining spillage in cloud computing
  - Defining a spillage chain
  - Defining use cases for the study of spillage
  - Providing examples of how the spillage chain and use cases to study the implications of spillage in cloud computing
  - Identifying recommendations

Definition of Spillage

HS SEDI
Homeland Security Systems Engineering and Development Institute

- **Considered data leakage/spillage definitions from CNSS-079-07; SANS: 20 Critical Security Controls, and NIST SP 800-53, Rev 4 (Draft)—NIST definition most appropriate**

Information spillage refers to instances where sensitive information (e.g., classified information, export-controlled information) is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, corrective action is required. The nature of the organizational response is generally based upon the degree of sensitivity of the spilled information (e.g., security category or classification level), the security capabilities of the information system, the specific nature of contaminated storage media, and the access authorizations (e.g., security clearances) of individuals with authorized access to the contaminated system.

*From NIST SP 800-53, Rev 4 (Draft)

Policy/Guidance Review

Summary of Policy/Guidance

Source	Related Cloud Computing Summary
NIST 800-53	Defines Security controls for Non-classified Federal information systems -Provides controls for three different risk levels (Low, Moderate, and High) -Number of controls increase as the risk level increases (Low is ~101, M ~174, & H ~215) -Divides controls into 18 security families; **No specific security controls for Cloud Computing**
FedRAMP	Lists the security controls and corresponding enhancements that Federal Agencies and Cloud Service Providers (CSPs) must implement within a cloud computing environment to satisfy FedRAMP requirements. **The security controls and enhancements have been selected from the NIST SP 800-53 Revision 3 catalog of controls.** The selected controls and enhancements are for systems designated at the low and moderate impact information systems as defined in the Federal Information Processing Standards (FIPS) Publication 199.
NIST 800-144	States a public cloud is one in which the infrastructure and computational resources that it comprises are made available to the general public over the Internet. **It is owned and operated by a cloud provider delivering cloud services to consumers and, by definition, is external to the consumers' organizations.** - Provides security & privacy recommendations in the following areas (Governance, Compliance, Architecture, I&A Mgmt, Trust, S/W Isolation, Data Protection, Availability, & Incident Response)
CSA	Lists the **top seven threats to Cloud Computing Implementations**: Threat #**1**: Abuse and Nefarious Use of Cloud Computing, Threat #**2**: Insecure Interfaces and APIs, Threat #**3**: Malicious Insiders, Threat #**4**: Shared Technology Issues, Threat #**5**: **Data Loss or Leakage,** Threat #**6**: Account or Service Hijacking, Threat #**7**: Unknown Risk Profile
DHS 4300a	Based upon the NIST 800-53 security controls, but **does not specifically address Cloud Computing** or Virtualization security issues.

Literature Review

Cloud Computing Complicates Clean-Up

- **Cloud-based office automation**
  - Document storage is ‘in the cloud’ outside organization’s boundary
  - Cleaning more difficult than for data on a user’s computer
- **Cloud-based collaboration services**
  - Collaboration tools store data ‘in the cloud’ outside organization’s boundary
  - Cleaning more difficult than for data on an organization’s internal servers
  - Possibility of collateral contamination of provider or other consumer resources
- **Cloud-based search**
  - Often use inverted indices that include all terms in the source document
  - Index may be contaminated by a data spill
  - Cleaning the index may be more difficult than cleaning the data
  - Cleaning the index may affect system availability and performance

Literature Review

Should the Provider be Informed?

- **Traditional advice: Do NOT tell the Internet Service Provider there has been a spill**
  - Limit knowledge of spill to contain impact
- **Cloud service providers offer services that include long-term persistent storage**
  - Can this be effectively cleaned without provider involvement?
  - The answer to this question may depend on the service model and the provider's specific implementation of the service model
  - IaaS and PaaS
    - Provider may not need to be informed if cleaning virtual storage resources is effective
    - Specifics on virtual-to-physical resource relationships may affect effectiveness
      - Understanding these relationships requires information from the provider
  - SaaS
    - Detailed knowledge of application implementation details needed to determine cleaning approach
    - Provider involvement likely necessary

Literature Review

Observations (1 of 2)

- **Academic research focuses on**
  - Preventing spills by reducing the likelihood of user mistakes that result in data spills
  - Tracing a spill back to the person responsible
- **Commercial products focus on**
  - Marking information to indicate sensitivity
  - Preventing spills using filtering technologies at organizational boundaries
- **Government guidance focuses on**
  - Assessing the scope and impact of a spill
  - Eradicating spilled data

Literature Review

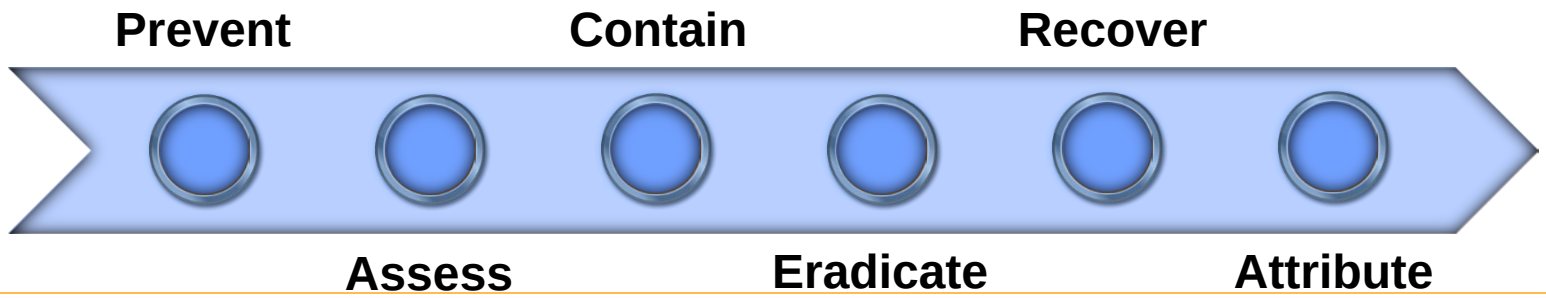
Observations (2 of 2)

- **Cloud computing**
  - Blurs or eliminates boundaries potentially reducing effectiveness of filtering technologies
  - Complicates assessing scope and impact of a spill due to possible collateral contamination of other cloud consumers with no relationship to the government
  - Complicates the eradication of spilled data due to potential need to involve the provider and other consumers affected by collateral contamination
- **Prevention should receive more emphasis**
  - Use of spill prevention techniques may be more important because of the impact of cloud computing on remediation techniques

Spill Chain for Analyzing Spillage Activities

HS SEDI
Homeland Security Systems Engineering and Development Institute

- **Prevent:** Reduce the likelihood of user mistakes that can lead to a spill.
- **Assess**: Determine whether a data spill has actually occurred, the sensitivity of the information potentially compromised, and the number of users, systems and applications involved.
- **Contain**: Identify all information hardware and software systems and applications affected, and execute approved procedures to ensure that the data spilled does not propagate further.
- **Eradicate**: When authorized execute approved sanitization procedures using approved utilities to permanently remove the data spilled from contaminated information systems, applications, and media.
- **Recover**: Use a clean backup media, as-built documentation and approved procedures to recover and restore all affected information systems and applications to an accredited, secure configuration.
- **Attribute**: Determine the source of the spill and take remedial action



Sample Use Cases for Analyzing Spillage in the Cloud

Use Case	Description
Web-based Desktop	Web-based desktop environment or applications. Google mail/apps is an example.
Storage	Storing data in cloud environment as a means for long term record retention or for disaster recovery. Carbonite is example.
Big Data Analytics	Big data analytics distributed across large computation systems. Examples include physics calculations for CERN or weather calculations for NOAA.
Knowledge Systems for Data	Storage and retrieval using meta data and search engines. Examples include library of congressional testimony and Lexis/Nexis.
Inter-Agency Collaboration	Using resources that are temporarily necessary for business partners or other agency collaborations.

Example

Spill Chain for Analyzing Web-Based Desktop

	Public SaaS Implementation
Prevent	• Provider must implement prevent capabilities within the desktop applications
Assess	• Provider participation required • Other consumer participation may be required
Contain	• Provider participation required
Eradicate	• Provider participation will be required to provide implementation information needed to determine if user-level cleaning is adequate
Recover	• Provider will likely have to perform recovery operations • Other consumers may be affected by recovery operations
Attribute	• May require capabilities within the desktop applications to include attribution information in documents and e-mail • Provider participation may be required

Example

Spill Chain for Analyzing Storage

	Public SaaS Implementation
Prevent	• Provider must implement privacy capabilities such as encryption within the storage software (in rest and transit)
Assess	• Provider participation required • Other consumer participation may be required
Contain	• Provider participation required • Other consumers may be impacted
Eradicate	• Provider participation will be required to provide implementation information needed to determine if user-level cleaning is adequate
Recover	• Provider will likely have to perform recovery operations • Other consumers may be affected by recovery operations
Attribute	• May require capabilities within the storage software to track attribution characteristics (username/password, PIV/CAC) • Provider participation may be required

Example

Spill Chain for Analyzing Big Data Analytics

	Community PaaS Implementation
Prevent	• Consumer or community member must implement security prevention capabilities within applications, such as access control on libraries
Assess	• Consumer and provider participation required • Other community member participation may be required
Contain	• Consumer and provider participation required
Eradicate	• Consumer and provider participation will be required to work together on implementation of eradication procedures
Recover	• Consumer and provider have to work together to perform recovery operations • Other community members may be affected by recovery operations
Attribute	• Consumer and provider participation work together.

Example

Spill Chain for Analyzing Knowledge Systems

	Community SaaS Implementation
Prevent	• Provider must implement prevent capabilities within the desktop applications
Assess	• Provider participation required • Other consumer participation may be required
Contain	• Provider participation required
Eradicate	• Provider participation will be required to provide eradication procedures, and implement clean up within provider control
Recover	• Provider will likely have to perform recovery operations • Other community members may be affected by recovery operations
Attribute	• May require capabilities within the search and data capabilities to include attribution information, such as username and passwords • Provider participation may be required

Example

Spill Chain for Analyzing Inter-Agency Collaboration

	Community IaaS Implementation
Prevent	• Consumer or community member must implement security prevention capabilities within applications, such as access control on libraries
Assess	• Consumer and provider participation required • Other community member participation may be required
Contain	• Consumer and provider participation required
Eradicate	• Consumer and provider participation will be required to work together on implementation of eradication procedures
Recover	• Consumer and provider have to work together to perform recovery operations • Other community members may be affected by recovery operations
Attribute	• Consumer and provider participation work together.

Example

Spill Chain for Analyzing NIST 800-53 Control Areas

Spill Chain Elements	Security Control Areas (As Defined by NIST 800-53)
Prevent	• Access Control (AC): Defines who or what is granted permission to access to a system or system component (especially on security enforcement) • Configuration Management (CM): Documents the proper configuration for the system and its components to support its mission and protect itself from harm
Assess	• Audit and Authorization (AU): Identifies if a data spillage occurred and the users (who or what) involved
Contain	• System Connectivity (SC): Identifies what external systems and information were potentially affected • System and Information Integrity (SI): Identifies what internal systems, information sets, and components were potentially affected
Eradicate	• Incident Response (IR): Defines the organization's response to a spill
Recovery	• Contingency Planning (CP): Defines the process for responding to identified data/system loss scenarios
Attribution	• Identification and Authentication (IA): Identifies who or what caused the spill

Example

Use Cases for Analyzing the Impact on Security Controls

Use Case Name	Applying Security Control: AC-5 Separation of Duties
Web-based Desktop	Partial – Expectation is the application and the underlying system infrastructure will play roles in addressing this control. For example, the application could provide user authentication and the system provide the reduction of the system audits.
Storage	Partial – Expectation is the environment (e.g., the data farm) would track when data was delivered/stored, but the application ISSO would be responsible for maintaining an inventory of what was stored.
Big Data Analytics	Fully – Expectation is the application would completely address the security concerns. This is important information whose integrity must be maintained.
Knowledge Systems for Data	Not Addressed – Expectation is the application or environment does not address this security concern. As they don't validate the data, they may rely on others to implement security duties.
Inter-Agency Collaboration	Partial – The security duties would be identified and shared per the Information Security Agreement (ISA).

The applied rating system is:
Fully –used when the application or environment is expected to completely address/resolve the security control,
Partial - used if the application or environment requires assistance from another source (e.g., another application or the environment), and
Not Addressed – used if the application or environment has no expectation to address/resolve the security control.

Recommendations

- **Refine draft use cases for typical government use of cloud computing**
- **Identify cloud service/deployment model combinations that can support each use case, e.g.**
  - Web-based desktop environment
    - Public or Community SaaS
- **Determine how each activity in the Spill Chain is affected by each service/deployment model combination for each use case**
- **Develop guidance based on the results on this analysis**

Roger Seeholzer
Information Security Office
US Department of Homeland Security

THANK YOU QUESTIONS?

SUPPLEMENTAL MATERIAL

Policy/Guidance Review

Reviewed Documents

- Homeland Security Presidential Directive 12 (HSPD-12): Policy for a Common Identification Standard for Federal Employees and Contractors (dated 27 August 2004)
- Data Leakage – Threats and Mitigation (Published by the SANS Institute InfoSec Reading Room, 15 Oct 2007)
- SANS: 20 Critical Security Controls (Version 3.1), Critical Control 17: Data Loss Prevention (www.sans.org, viewed 9 Jul 12)
- NIST Special Publications 800-53, Recommended Security Controls for Federal Information Systems and Organizations (Rev 3, August 2009)
- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (24 Jan 2012)
- DHS 4300A, DHS Sensitive Systems Policy Directive 4300A (Version 8.0, 14 Mar 2011)
- DHS Security Architecture Appendix: Secure Cloud Computing (Draft Version 0.13, 17 May 2012)
- Cloud Security Alliance published cloud security documents (e.g., Top Threats to Cloud Computing v1.0, 2010; Security Guidance, 2011; Cloud Controls Matrix, 2011)
- Virtualization Security Best Practices, DHS OCIO ESDO (Jan 2010)
- CNSS-079-07, August 2007, Frequently Asked Questions (FAQ) on Incidents and Spills

Literature Review

Relevant Articles

- Ankit Argarwal, Mayur Gaikwad, Kapil Garg, and Vahid Inamdar; ***Robust Data Leakage and Email Filtering System***; 2012 International Conference on Computing, Electronics and Electrical Technologies.
- S. Subashini and V. Kavitha; ***A Survey on Security Issues in Service Delivery Models of Cloud Computing***; Journal of Network and Computer Applications 34 (2011) 1-11.
- Qihua Wang and Hongxia Jin; ***Data Leakage Mitigation for Discretionary Access Control in Collaboration Clouds***; Association for Computing Machinery 2011.
- Stan Wisseman; ***Cloud Computing Security***; Booz, Allen, and Hamilton; December 9, 2009.
- Committee on National Security System (CNSS); ***National Instruction on Classified Information Spillage; CNSS Instruction No. 1001; February 2008.***
- Panagiotis Papdimitriou and Hector Garcia-Molina; ***Data Leakage Detection***; IEEE Transactions on Knowledge and Data Engineering; Vol. 23; No. 1; January 2011.
- George Lawton; ***New Technology Prevents Data Leakage***; IEEE Computer Society; September 2008.
- Sarah Jane Hughes; ***Payments Data Security Breaches and Oil Spills: What Lessons Can Payments Security Learn from the Laws Governing Remediation of the Exxon Valdex, Deepwater Horizon, and Other Oil Spills?***; Maurer School of Law: Indiana University; January 1, 2010.
- Igor Burdonov, Alexander Kosachev, and Pavel Iakovendo; ***Virtualization-Based Separation of Privilege: Working with Sensitive Data in Untrusted Environments***; Association of Computing Machinery; March 31, 2009.
- Anna Squicciarini; Smitha Sundareswaran; and Dan Lin; ***Preventing Information Leakage from Indexing in the Cloud***; 2010 IEEE 3rd International Conference on Cloud Computing.
- CNSS, ***Frequently Asked Questions (FAQ) on Incidents and Spills***; CNSS-079-07; August 2007.
- www.jpwsec.com; ***Dealing with Data Spillages***; Downloaded July 20, 2012.

Policy/Guidance Review

Selected Security Controls Spillage in Cloud Computing (1 of 2)

Security Controls		Security Controls	
AC-1	Access Control Policy and Procedures	IA-1	Identification and Authentication Policy and Procedures
AC-3	Access Enforcement	IA-3	Device-to-Device Identification and Authentication
AC-4	Information Flow Enforcement	IA-5	Authenticator Management
AC-5	Separation of Duties	IA-7	Cryptographic Module Authentication
AC-7	Unsuccessful Login Attempts	IR-1	Incident Response Policy and Procedures
AC-10	Concurrent Session Control	IR-3	Incident Response Testing
AC-17	Remote Access	IR-5	Incident Monitoring
AC-22	Publicly Accessible Content	IR-8	Incident Response Plan
AU-1	Audit and Accountability Policy and Procedures	IR-9	Information Spillage Response
AU-3	Content of Audit Records	SC-1	System Connectivity Policy and Procedures
AU-5	Response to Audit Processing Failures	SC-3	Security Function Isolation
AU-7	Audit Reduction and Report Generation	SC-5	Denial of Service Protection
AU-9	Protection of Audit Information	SC-8	Transmission Integrity
AU-11	Audit Record Retention	SC-10	Network Disconnect
CM-1	Configuration Management Policy and Procedures	SC-`13	Cryptographic Protection
CM-3	Configuration Change Control	SC-15	Collaborative Computing Devices
CM-5	Access Restrictions for Change	SC-18	Mobile Code
CM-4	Security Impact Analysis	SC-24	Fail in Known State
CM-7	Least Functionality	SC-32	Information System Partitioning
CM-9	Configuration Management Plan	SC-41	Process Isolation
CP-2	Contingency Plan	SI-2	Flaw Remediation
CP-4	Contingency Plan Testing	SI-4	Information System Monitoring
CP-7	Alternate Processing Site	SI-6	Security Function Verification
CP-9	Information System Backup	SI-7	Software, Firmware, and Information Integrity
CP-11	Predictable Failure Prevention		

Policy/Guidance Review

Selected Security Controls Spillage in Cloud Computing (2 of 2)

- **Selected moderate-impact NIST 800-53, Rev 3 and Rev 4 security controls relevant to spillage in the cloud using:**
  - DHS Virtualization Security Best Practices recommendations
  - SANS Critical Control 17: Data Loss Prevention
  - Review of new controls in NIST 800-53, Rev 4