Cloud Security and Cloud Compliance

Cloud Security services and mechanisms:
How can modern clouds provide secure and trusted environment for data and business applications?

Yuri Demchenko
Systems and Networking Lab, University of Amsterdam

Amsterdam Security Workshop
9 Oct 2019, UvA
Outline

• Introduction: Cloud adoption is growing
• Shared Responsibility Security Model in Cloud
• Case Study: AWS Security
• Cloud Compliance and Cloud Security Alliance (CSA)
  – CSA GRC Stack: Governance, Risk Management and Compliance
  – Consensus Assessment Initiative Questionnaire (CAIQ)
• DevSecOps = DevOps + SSDL (Security Services Development Lifecycle)
• Case Study: Trusted Data Market infrastructure and IDS Connector
• Discussion: Research topics in Cloud Security and Trust
Cloud Adoption is Growing

- Cloud adoption is growing: Enterprise Cloud Strategy 2019

![Enterprise Multi-Cloud Strategy YoY](http://googliers.net/static/media/uploads/download_files/2019_state_of_the_cloud_report.pdf)

Source: RightScale 2019 State of the Cloud Report from Flexera
Cloud Facts and Observations: AWS vs Azure

- Microsoft Azure is fastest growing cloud: now 85% of AWS (compare 70% in 2018)
- Quite popular in Netherlands
Cloud Observations

- Cloud is an ultimate platform for Big Data
  - Data gravity vs Investments gravity
    - Migration choice: 10 yrs of legacy data vs expected explosive data growth
  - Working with data and data analytics in cloud is much easier
    - Hybrid cloud and data analytics solution is growing
    - **Data Lakes**: heterogeneous data formats, namespaces, filesystems

- Migration to cloud takes 1-2 years, requires competence planning
  - Demand for cloud migration/integration services/companies
  - Growing adoption of the DevOps culture in services development and operation

- Most of new projects are in cloud
Part 1: Cloud Security and AWS Example

- Shared responsibility model
- AWS Security
Security management responsibilities split between Customer and Provider for IaaS, PaaS, SaaS service models

- Updating firmware and software for platform and for customer managed components
- Firewall is intrusion prevention and a responsibility of the cloud provider
- Certification and compliance of the cloud platform doesn't imply security and compliance of the customer controlled components
Cloud Computing Security – Challenges

• Fundamental security challenges and main user concerns in clouds
  – Data security: Where are my data? Are they protected? What control has cloud provider over data security and location?
  – Identity management and access control: Who has access to my personal/ID data?

• Two main tasks in making cloud secure and trustworthy
  – Secure operation of the cloud (provider) infrastructure
  – User controlled access control (security) infrastructure
    • Provide sufficient amount of security controls for competent user

• Security services are provisioned **on-demand** (as part of virtualised infrastructure) and require **bootstrapping (federation)** with the customer services and trust domain
Cloud, OS, Network and Applications Trust Layers

- Consistent security must provide security at all layers correspondingly relying on trust credentials at each layer
  - Application – Container - Operating systems (security kernel) + Cloud platform
  - Network/communication – Runtime - Storage
- Two security models: Trusted Computing Base (TCB) for cloud platform and OSI/Internet security cloud based applications
  - Client/server and Service Oriented Architecture vs OS and hypervisor run-time
- Root of trust is based on the security credentials bound to hardware mediated through OS to runtime environment
Multi-tenant Application: Example Implementation

Microsoft Azure Cloud

Tenant A
- Web UI
  - Client A
    - Single tenant

Tenant B
- Web UI
  - Client B
    - Single tenant

Tenant C
- Web UI
  - Client C
    - Single tenant

App Services Multi-tenant
- Data processing

Storage Partition
- Client A
  - Single tenant
- Client B
  - Single tenant
- Client B
  - Single tenant

Data transformation in multi-tier multi-tenant applications

Data Source and Consumer

Data input/output

Data storage

Access control

Processing threads isolated

Data separation

Generally reflects Office 365 multitenancy model
Designing for Multi-tenancy in Cloud - Overview

- Data security and privacy is a primary concern and design target in multi-tenant applications
  - Cloud datacenter security – ensured by cloud provider
  - Application security – ensured by the application developer and service operator
- Multi-layer and multi-tier multi-tenancy mechanism
  - Presentation, business logic, data structures
- Data isolation and segregation
  - Store client data with isolated URI or schema -> Data Lakes
  - Blob or Table storage: isolated URI
  - Azure SQL database: partitioning, separate schema
- Access control and Identity management
  - Microsoft Azure Active Directory and Windows Identity Foundation
  - AppFabric Access Control
  - Identity federation with the tenants’ home organisations
  - Custom Identity Solution
- Scalability up and down, horizontal scalability
- Services metering, accounting and billing
Case Study: AWS Security Mechanisms

- VPC – Virtual Private Cloud
  - VPN – Virtual Private Network
  - VPG – VPN Private Gateway
  - IGW – Internet Gateway
- HTTPS and TLS/SSL, SSH, KPI
- AIM – Access and Identity Management
- Other security services
  - AWS SSO
  - Cognito – Identity Federation
  - Macie - Data visibility security service
  - CloudHSM - Managed hardware security module (HSM)
Example: Security responsibility sharing in AWS IaaS infrastructure services

- For other cloud service models PaaS and SaaS the responsibility of AWS goes up to OS, network and firewall for PaaS, and also includes the application platform and container for SaaS.
  - However, the responsibility for data remains with the customer.

Security is declared as one of critical importance to AWS cloud that is targeted to protect customer information and data from integrity compromise, leakage, accidental or deliberate theft, and deletion.

- The AWS infrastructure is designed with the high availability and sufficient redundancy to ensure reliable services operation.
Microsoft Azure Active Directory (AAD) provides 4 basic services:

- **Microsoft Azure AD Access Control (ACS)**
  - Centralized authentication and authorization hub

- **Microsoft Azure AD Directory**
  - Cloud-based identity store / provider

- **Microsoft Azure AD Graph**
  - Developer Restful API for the cloud directory

- **Microsoft Azure Authentication Library (AAL)**
  - Developer library to make authentication in Azure apps easy

Microsoft Azure Active Directory is a modern cloud service providing Identity Management and Access Control capabilities to cloud applications.

- Provides Identity and access management in the cloud
- Can be integrated with on-premises AD
- Supports Integration with cloud applications
Microsoft Azure AD Access Control

• A cloud federation service for your cloud applications and services
  – Federates on-premises and cloud identity services

• Prerequisites
  – Demands federated authentication
  – AD on-premises and AAD on cloud synchronisation

• Supports multiple identity providers
  – Facebook, Google, Microsoft, Windows Server AD FS, Yahoo!

• Supports multiple protocols
  – WS-Federation, WS-Trust, OAuth 2.0 (draft 13)

• Supports multiple tokens
  – JWT, SAML 1.1/2.0, SWT
Part 2. Cloud Compliance

- Compliance standards, Security Controls
- CSA GRC Stack: Governance, Risk Management and Compliance
- Compliance Assessment Initiative Questionnaire (CAIQ)
Security and Compliance

- Security and compliance are related and in some cases interchangeable

- **Security** is commonly defined as a set of technical, physical, and administrative controls in order to ensure normal operation of a system or application
  - Security is often associated with the CIA triad Confidentiality, Integrity, Availability
  - Appropriate level of security requires organizations to take measures and comply to the numerous security controls

- **Compliance** is a certification or confirmation that the system or an organization meets the requirements of specified standards, established legislation, regulatory guidelines or industry best practices that can be jointly defined as compliance framework
  - A compliance framework can includes business processes and internal controls the organization has in place to adhere to these standards and requirements
  - The framework should also map different requirements to internal controls and processes to eliminate redundancies

- **Why it is important for cloud?**
  - When moving to cloud, the organization moves from internal security and operational environment/context (that may not be formally defined) to external operational security that will become a part of SLA (or business requirement) with CSP

- **Problem with achieving compliance for cloud based applications/solutions**
  - Audit requirements are not designed for virtualised distributed environment
  - Lack of visibility in cloud: large CSP such as Amazon and Google are “walled/curtained gardens”
  - Requirements to allow CSP audit may involve Non-Disclosure Agreement (NDA) and risk of provider lock-in
Regulatory requirements to be considered for cloud compliance – Example General Standards

General standards and recommendations

- ISO/IEC 27001:2005 Certification on security infrastructure
  - Industry standard: the risk-based information security management program that follows a plan-do-check-act process
- NIST SP 800-53 Security Controls and ISO/IEC 15408 Evaluation Criteria
- HIPAA/HITECH - The U.S. Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH)
  - Act created by the US federal government include provisions to protect patients' private information.
- NIST SP 800-144 Guidelines for Security and Privacy in Cloud Computing
- ENISA Cloud Computing Security Risk Assessment
- GDPR (General Data Protection Regulation)
The AWS cloud infrastructure has been designed and managed in alignment with regulations, standards, and best-practices including:

- ISO/IEC 27001:2005
- SOC 1, SOC2, SOC3
- FIPS 140-2
- CSA
- PCI DSS Level 1
- HIPAA
- ITAR
- DIACAP and FISMA
- FedRAMP (SM)
- MPAA

Amazon Cloud is certified for hosting US Governmental services

http://aws.amazon.com/compliance/
Microsoft services/infrastructure meets the following key certifications, attestations and compliance capabilities:

- Current Compliance Offerings
- Office 365 Compliance Documentation
- Service Trust Portal
- Microsoft Services Risk Assessment
- Audit Reports

Microsoft has certified its current compliance capabilities through the following frameworks and standards:

**Global Standards**

<table>
<thead>
<tr>
<th>Global Standards</th>
<th>Government</th>
<th>Industry</th>
<th>Regional</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS Benchmark</td>
<td>CJIS</td>
<td>23 NYCRR Part 500</td>
<td>BIR 2012 (Netherlands)</td>
</tr>
<tr>
<td>CSA Cloud Control Matrix</td>
<td>CNSSSI 1253</td>
<td>AFM + DNB (Netherlands)</td>
<td>CS (Germany)</td>
</tr>
<tr>
<td>CSA-STAR-Attestation</td>
<td>DFARS</td>
<td>APRA (Australia)</td>
<td>CCSL/IRAP (Australia)</td>
</tr>
<tr>
<td>CSA-Star-Certification</td>
<td>DoD DISA L2, L3, L5</td>
<td>AMF and ACPR (France)</td>
<td>CS Mark (Gold) (Japan)</td>
</tr>
<tr>
<td>CSA STAR Self-Assessment</td>
<td>DoE 10 CFR Part 810</td>
<td>CDSA</td>
<td>Cyber Essentials Plus (UK)</td>
</tr>
<tr>
<td>ISO 20000-1:2011</td>
<td>EAR (US Export Administration Regulations)</td>
<td>CFTC 1.31 (US)</td>
<td>Canadian Privacy Laws</td>
</tr>
<tr>
<td>ISO 22301</td>
<td>FedRAMP</td>
<td>DPP (UK)</td>
<td>DJCP (China)</td>
</tr>
<tr>
<td>ISO 27001</td>
<td>FIPS 140-2</td>
<td>EBA (EU)</td>
<td>EN 301 549 (EU)</td>
</tr>
<tr>
<td>ISO 27017</td>
<td>IRS 1075</td>
<td>FACT (UK)</td>
<td>ENS (Spain)</td>
</tr>
<tr>
<td>ISO 27018</td>
<td>ITAR</td>
<td>FCA (UK)</td>
<td>ENISA IAF (EU)</td>
</tr>
<tr>
<td>ISO 27701</td>
<td>NIST 800-171</td>
<td>FDA CFR Title 21 Part 11</td>
<td>EU-Model-Clauses</td>
</tr>
<tr>
<td>ISO-9001</td>
<td>NIST Cybersecurity Framework (CSF)</td>
<td>FERPA</td>
<td>EU-U.S. Privacy Shield</td>
</tr>
<tr>
<td>SOC 1</td>
<td>Section 508 VPATS</td>
<td>FFIEC (US)</td>
<td>GB 18030 (China)</td>
</tr>
<tr>
<td>SOC 2</td>
<td></td>
<td>FINMA (Switzerland)</td>
<td>GDPR (EU)</td>
</tr>
</tbody>
</table>

For more information, visit: [https://www.microsoft.com/en-US/TrustCenter/Compliance/complianceofferings](https://www.microsoft.com/en-US/TrustCenter/Compliance/complianceofferings)
Cloud Security Alliance (CSA) GRC Stack: Governance, Risk Management and Compliance

The GRC Stack provides a toolkit for enterprises, cloud providers, security solution providers, IT auditors and other stakeholders to assess both private and public clouds against industry established best practices, standards and critical compliance requirements. [https://cloudsecurityalliance.org/research/grc-stack/](https://cloudsecurityalliance.org/research/grc-stack/)

- **Cloud Controls Matrix (CCM)** is designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider ([https://cloudsecurityalliance.org/research/ccm/](https://cloudsecurityalliance.org/research/ccm/))
  - The CCM gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains
  - Defined in accordance to industry-accepted security standards, regulations, and controls frameworks such as the HITRUST CSF, ISO 27001/27002, ISACA COBIT, PCI, HIPAA and NIST.

- **Consensus Assessments Initiative Questionnaire (CAIQ)** provides an industry-accepted way to document what security controls exist in IaaS, PaaS, and SaaS offerings, providing security control transparency ([https://cloudsecurityalliance.org/research/cai/](https://cloudsecurityalliance.org/research/cai/))
  - Provided in a form of questionnaire in the spreadsheet format, a set of questions a cloud consumer and cloud auditor may wish to ask of a cloud provider.
  - ~ 200 yes/no questions that map directly to the CCM, and thus, in turn, to many industry standards.
  - **CAIQ answers by companies and certification are posted on the STAR website**
    - From self-assessment to certification and monitoring
The CSA3.0 defines 13 domains of the security concerns (controls) for Cloud Computing that are divided into two broad categories that define corresponding security controls.

**Governance domains**
1. Governance and Enterprise Risk Management
2. Legal Issues: Contracts and Electronic Discovery
3. Compliance and Audit
4. Information Management and Data Security
5. Portability and Interoperability

**Operational Domains**
6. Traditional Security, Business Continuity and Disaster Recovery
7. Data Center Operations
8. Incident Response, Notification and Remediation
9. Application Security
10. Encryption and Key Management
11. Identity and Access Management
12. Virtualization
13. Security as a Service
CSA3.0: Mapping the Cloud Model to the Security Control & Compliance

Cloud Model

Security Control Model

- Applications: SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
- Information: DLP, CMF, Database Activity Monitoring, Encryption
- Management: GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
- Network: NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
- Trusted Computing: Hardware & Software RoT & API's
- Compute & Storage: Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
- Physical: Physical Plant Security, CCTV, Guards

Compliance Model

- PCI
  - Firewalls
  - Code Review
  - WAF
  - Encryption
  - Unique User IDs
  - Anti-Virus
  - Monitoring/IDS/IPS
  - Patch/Vulnerability Management
  - Physical Access Control
  - Two-Factor Authentication...

ISO/IEC 27002:2013 InfoSec Controls
(Historically originated from Common Criteria)

SP500-292 (CCRA), CSA3.0

Recent CSA Publications

• **Top Threats to Cloud Computing: The Egregious 11 (2019)**
  – Contains stories about recent cloud breaches: all due to customer lame design and compromised credentials

• **Top Threats to Cloud Computing: Deep Dive (2019)**
  – A case study analysis for The Treacherous 12 Top Threats to Cloud Computing and relative industry breach analysis

• **The Six Pillars of Security (2019)**
  – Achieving Reflexive Security through integration of security < development and Operations

• **Cloud Octagon Model (2019)**
  – Model for Improving Accuracy and Completeness of cloud Computing risk assessment
DevSecOps and SSDL

- SSDL – Security Services Development Lifecycle
  - Developed by Microsoft in 2000s and widely accepted by industry

SSDL = Security and Privacy by Design

- Security design principles by big software vendors Amazon, Apple, Google

- DevOps meets Security -> DevSecOps
- DevSecOps as alternative to Waterfall model where security is treated as non-functional requirement and is addressed at later stages of development
DevSecOps: Building a Secure Continuous Delivery Pipeline

• DevSecOps is extension of DevOps with inclusion of Security
• Traditional InfoSec crisis: Lost identity
  – 100 developers:10 operations:1 security -- problem
• Continuous delivery pipeline and DevSecOps toolchain: 5 stages
  – Develop: version, sprint, unit test
  – Inherit: libraries and dependencies
  – Build: acceptance testing, audit
  – Deploy (moving artefact from built machine to production)
  – Operate: user and attacker faced
Security Testing: Misconfiguration and secrets

- Creds leakage, e.g.
  - Creds in source code on github
  - AWS access key in a version control history
- Use **git-secrets**
  https://github.com/awslabs/git-secrets
  - Prevents from committing passwords and other sensitive information to a git repository
  - `git-secrets` scans commits, commit messages, and --no-ff merges to prevent adding secrets into your git repositories.
  - If a commit, commit message, or any commit in a --no-ff merge history matches one of your configured prohibited regular expression patterns, then the commit is rejected.
  - Installation for Linux, Mac, Windows
- Use: `git secrets --scan[-history]`
Security Development Practices and OSS

• Security of Open Source Software (OSS) is slightly agitated
  – Security problems require security expertise and not all developers are security experts.
    • More advanced topics like cryptography, for example, further narrow the field for those who can review code for such security flaws.
  – There's also no standard way of documenting security on open source projects. In the top 400,000 public repositories on GitHub, only 2.4% had security documentation in place.
  – Dependencies in open source projects allow some vulnerabilities to fly under the radar..

• According to the latest Veracode report, only 28% of organizations do any kind of regular analysis to find out what components are built into their applications.
  – 94% commercial software have dependencies on OSS libraries
  – As the use of open source code grows, this risk surface expands.

• According to the Snyk survey (https://snyk.io):
  – 88 % of open source code maintainers add security-related announcements to the release notes
  – 34 % say that they deprecate the older, insecure version.
  – 25% that they make no effort at all to notify users of vulnerabilities
  – only 10% file a CVE reports
Cloud Security Config Monitoring

- **AWS Tools**
  - AWS Config – Monitor configuration changes
  - AWS CloudTrail - Create a trail to retain a record of events
  - Amazon Inspector - analyzes the behavior of AWS resources and helps identify potential security issues
  - Amazon GuardDuty – Activity monitoring & Intelligent threat detection

- **Third party tools**
  - https://www.threatstack.com
  - https://www.alienvault.com
  - https://evident.io – multicloud solution

- **InSpec** is compliance as code service https://www.inspec.io
  - Turns compliance, security, and other policy requirements into automated tests
  - Includes compliance requirements into code
Case Study: Trusted Data Market Infrastructure and composable components

Operational Trusted DM Platform
Component/services
Open Telekom Cloud (OTC)

Catalog/Directory (Federated)

Data Lake Store

Template/Image
Virtual TDM od

Template VPC

Template/Image
SecDataCont

Data Intel Hub
Compute

Deployment Engine

FedAAI

SLAM

SmartContract/Policy

SCVPE4TDM (EVM)

Legal/Rules

Private
VDM

VI TBP (TPM)

Sealed Room

Trusted Broker
(3rd Party)

Data

## Data Providers

Data

## Users

Data

KPI

$$$ Data Exchange

### Transactions

KPI

## Data Providers

Data

## Users

Data

IDS

IDS

IDS

IDS

IDS

IDS

IDS

IDS

IDS

IDS

IDS
TDM Infrastructure Templates and DevOps tools

• DM infrastructure is provisioned on demand for each cooperating groups of partners
  – Digitally Enforceable Policy/Contract is embedded into infrastructure

• DM infrastructure template is composed of basic infrastructure patterns described
  – For platform dependent patterns in the formats of cloud platform
    • AWS: CloudFormation
    • Azure: Azure Resource Manager (ARM)
  – For general infrastructure descriptions/templates
    • Ansible – YAML based, combines computational and network resources
    • Others: Chef (directly supported by AWS), Puppet, Terraform (directly supported by Azure)
  – Blockchain enabled Virtual Private execution Engine (SCVPE)
Leveraging IDS Architecture and Connector with Cloud

- IDS Connector is the main functional component
- No specifically defined infrastructure
Reference Architecture Data Connector

- Execution and configuration
- Application container

- Undergoing DIN Standardisation
The Trusted Connector features the secure container management layer trust|me as an alternative to Docker.

- trust|me basic mechanisms are similar to Docker (namespaces, cgroups and chroot)
- trust|me was developed as a security architecture including secure boot, platform integrity measurements, and a hardened kernel.
Research topics in Cloud Security

• Federated Identity Management and Access Control in hybrid enterprise-CSP infrastructure + Identity provisioning

• Cloud Access and Security Brokers: Security with Trusted Third Party

• VPC infrastructure security model and analysis

• Bootstrapping cloud based VPC and enterprise or applications trust domains
  – Leveraging Zero Trust model in networking security
  – Leveraging TPM and Trusted Computing Platform Architecture

• Data protection in clouds at all stages of data processing (Data Lifecycle)
  – Data Sovereignty and Data Ownership attribute/property
  – Computationally Enforceable Policies and data provenance
  – Data Management Infrastructure for AI and Digital Twins
  – Blockchain enabled data provenance in multi-platform multi-cloud environment

• Personal information protection in cloud based multitenant multi-tier applications

• Cloud infrastructure to enable GDPR + FAIR data principles
Summary and take away

- Cloud Security impose new security challenges
- Cloud Security is based on the core security principles and models
- Shared responsibility is the basic model cloud security
- Cloud compliance provides a basis for wider cloud services adoption and inter-cloud integration.
- Compliance is supported by numerous standards, legislation, regulatory guidelines and industry best practices that jointly define a compliance framework
  - Knowing major cloud compliance standards is necessary for correct cloud services design, deployment and operation
- IDSA architecture and Trusted Data Market as example of critically trusted environment in cloud
Discussion and Questions