AWS: Overview of Security Processes

Bill Murray
Manager – AWS Security Programs
Certifications & Accreditations
- Sarbanes-Oxley (SOX) compliance
- ISO 27001 Certification
- PCI DSS Level I Certification
- HIPAA compliant architecture
- SAS 70(SOC 1) Type II Audit
- FISMA Low & Moderate ATOs
- DIACAP MAC III-Sensitive
  - Pursuing DIACAP MAC II-Sensitive

Shared Responsibility Model
- Customer/SI Partner/ISV controls
  - guest OS-level security, including patching and maintenance
- Application level security, including password and role based access
- Host-based firewalls, including Intrusion Detection/Prevention Systems
- Separation of Access

Physical Security
- Multi-level, multi-factor controlled access environment
- Controlled, need-based access for AWS employees (least privilege)

Management Plane Administrative Access
- Multi-factor, controlled, need-based access to administrative host
- All access logged, monitored, reviewed
- AWS Administrators DO NOT have logical access inside a customer's VMs, including applications and data

VM Security
- Multi-factor access to Amazon Account
- Instance Isolation
  - Customer-controlled firewall at the hypervisor level
  - Neighboring instances prevented access
  - Virtualized disk management layer ensure only account owners can access storage disks (EBS)
- Support for SSL end point encryption for API calls

Network Security
- Instance firewalls can be configured in security groups;
- The traffic may be restricted by protocol, by service port, as well as by source IP address (individual IP or Classless Inter-Domain Routing (CIDR) block).
- Virtual Private Cloud (VPC) provides IPSec VPN access from existing enterprise data center to a set of logically isolated AWS resources
Shared Responsibility Model

**AWS**
- Facilities
- Physical Security
- Physical Infrastructure
- Network Infrastructure
- Virtualization Infrastructure

**Customer**
- Operating System
- Application
- Security Groups
- Network ACLs
- Network Configuration
- Account Management

AWS Summit 2012 | Navigate the Cloud
AWS Security Resources

- Security Whitepaper
- Risk and Compliance Whitepaper
- Latest Versions May 2011, January 2012 respectively
- Regularly Updated
- Feedback is welcome
AWS Certifications

- Sarbanes-Oxley (SOX)
- ISO 27001 Certification
- Payment Card Industry Data Security Standard (PCI DSS) Level 1 Compliant
- SAS70(SOC 1) Type II Audit
- FISMA A&As
  - Multiple NIST Low Approvals to Operate (ATO)
  - NIST Moderate, GSA issued ATO
  - FedRAMP
- DIACAP MAC III Sensitive ATO
- Customers have deployed various compliant applications such as HIPAA (healthcare)
SOC 1
Type II – Control Objectives

- Control Objective 1: Security Organization
- Control Objective 2: Amazon Employee Lifecycle
- Control Objective 3: Logical Security
- Control Objective 4: Secure Data Handling
- Control Objective 5: Physical Security
- Control Objective 6: Environmental Safeguards
- Control Objective 7: Change Management
- Control Objective 8: Data Integrity, Availability and Redundancy
- Control Objective 9: Incident Handling
AWS has achieved ISO 27001 certification of our Information Security Management System (ISMS) covering AWS infrastructure, data centers in all regions worldwide, and services including Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3) and Amazon Virtual Private Cloud (Amazon VPC). We have established a formal program to maintain the certification.
Amazon has been building large-scale data centers for many years

Important attributes:
- Non-descript facilities
- Robust perimeter controls
- Strictly controlled physical access
- 2 or more levels of two-factor auth

Controlled, need-based access for AWS employees (least privilege)

All access is logged and reviewed
AWS Regions

- GovCloud (US ITAR Region)
- US West (Northern California)
- US West (Oregon)
- US East (Northern Virginia)
- South America (Sao Paulo)
- EU (Ireland)
- Asia Pacific (Singapore)
- Asia Pacific (Tokyo)

AWS Edge Locations
AWS Regions and Availability Zones

Customer Decides Where Applications and Data Reside
Amazon EC2 Security

Host operating system
- Individual SSH keyed logins via bastion host for AWS admins
- All accesses logged and audited

Guest operating system
- Customer controlled at root level
- AWS admins cannot log in
- Customer-generated keypairs

Firewall
- Mandatory inbound instance firewall, default deny mode
- Outbound instance firewall available in VPC
- VPC subnet ACLs

Signed API calls
- Require X.509 certificate or customer’s secret AWS key
Network Security Considerations

- **DDoS (Distributed Denial of Service):**
  - Standard mitigation techniques in effect

- **MITM (Man in the Middle):**
  - All endpoints protected by SSL
  - Fresh EC2 host keys generated at boot

- **IP Spoofing:**
  - Prohibited at host OS level

- **Unauthorized Port Scanning:**
  - Violation of AWS TOS
  - Detected, stopped, and blocked
  - Ineffective anyway since inbound ports blocked by default

- **Packet Sniffing:**
  - Promiscuous mode is ineffective
  - Protection at hypervisor level
Amazon Virtual Private Cloud (VPC)

- Create a **logically isolated** environment in Amazon’s highly scalable infrastructure
- Specify your **private IP** address range into one or more public or private subnets
- Control inbound and outbound access to and from individual subnets using stateless **Network Access Control Lists**
- Protect your Instances with stateful filters for inbound and outbound traffic using **Security Groups**
- Attach an Elastic IP address to any instance in your VPC so it can be reached **directly from the Internet**
- Bridge your VPC and your onsite IT infrastructure with an industry standard encrypted **VPN connection and/or AWS Direct Connect**
- Use a **wizard** to easily create your VPC in 4 different topologies
Amazon VPC Architecture

- Secure VPN Connection over the Internet
- AWS Direct Connect – Dedicated Path/Bandwidth
- Customer’s Network
- Amazon Web Services Cloud
- NAT
- VPN Gateway
- Router
- Customer’s isolated AWS resources
- Subnets
Amazon VPC - Dedicated Instances

- New option to ensure physical hosts are not shared with other customers
- $10/hr flat fee per Region + small hourly charge
- Can identify specific Instances as dedicated
- Optionally configure entire VPC as dedicated
# AWS Deployment Models

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercial Cloud</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>Public facing apps. Web sites, Dev test etc.</td>
</tr>
<tr>
<td>Virtual Private Cloud (VPC)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>Data Center extension, TIC environment, email, FISMA low and Moderate</td>
</tr>
<tr>
<td>AWS GovCloud (US)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>US Persons Compliant and Government Specific Apps.</td>
</tr>
</tbody>
</table>
Thanks!

Remember to visit
https://aws.amazon.com/security