Towards Least Privilege in the Cloud

Kevin Alejandro Roundy
Kevin@andromedasecurity.com
The Problem

A single identity with excessive privilege caused business impact

95% of privileges are excessive

Explosive growth in Human and Service Identities

10K+ permissions in Cloud and Apps
Let’s Log Into AWS
Let’s Log Into AWS

AWS Account
A cloud environment that contains data and resources

Policy
A set of Permissions (aka Actions) and the resources to which they apply
Group-Based Management

- For easy permissions management
  - Users -> Groups
  - Groups -> Roles
  - Roles -> Policies in specific Accounts

- Group examples
  - Cloud developers, cloud admins, data scientists, auditors, contractors, etc.

- Permission Creep
  - If any member of the group needs an additional permission, everyone in the group gets it

AWS Actions/Permissions

- 15,423 permissions and counting
- 367 distinct services
- 5 Access Levels: Tagging, List, Read, Write, Permission Mgmt
Kevin and other data scientists want to study data stored in S3 by running SQL queries through Athena.

- **ReadOnlyAccess** Policy (5000+ permissions)
- Athena requires **S3 Write access** as well for storing results.
Security Concerns

Excessive Privilege
- Does an identity have too many permissions?
- Are the permissions needed all the time? Have they used them?

Data governance
- Which accounts have sensitive data and where is it? Passwords in scripts?
- As more sensitive data gets added to an account, are permissions still correct?

Identity Management
- As employees join, change roles in the company, and leave, we need to manage their permissions.
- If not tracked properly, employees can access sensitive data after leaving the company or team

Blast Impact of Compromised Identity
- How much damage can an attacker do after account takeover? How can we measure this?
Our Castle in the Cloud: Least Privilege

Standing Privilege

Kevin’s Policies

- RDS
- S3
- VPC
- EC2
- App Flow
- Cloud Trail
- Neptune
- IAM
Move to Least Standing Privilege

Objectives:
Allow only low risk permissions that are regularly used
All other permissions only on as-needed basis

How should we measure risk and determine genuine need?
Modeling Risk

User or Account Risk

Risk of User in Account Across Policies

Policy Risk

Permission Risk

© 2023 Andromeda Security
**Permission Risk: 15,423 permissions to score**

<table>
<thead>
<tr>
<th>Access Level</th>
<th>But in reality...</th>
</tr>
</thead>
<tbody>
<tr>
<td>List</td>
<td>List, Read Tags</td>
</tr>
<tr>
<td>Tagging</td>
<td>Write Tag, Delete Tag</td>
</tr>
<tr>
<td>Read</td>
<td>Read Metadata, Read Data</td>
</tr>
<tr>
<td>Write</td>
<td>Create infra, Write, Write Metadata, Delete Data, Delete infra</td>
</tr>
<tr>
<td>Permissions Mgmt</td>
<td>Permissions Mgmt, Permissions viewing and reporting</td>
</tr>
</tbody>
</table>
### Permission Risk: 15,423 permissions to score

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Service Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>List</td>
<td></td>
</tr>
<tr>
<td>Tagging</td>
<td></td>
</tr>
<tr>
<td>Read</td>
<td></td>
</tr>
<tr>
<td>Write</td>
<td></td>
</tr>
<tr>
<td>Permissions Mgmt</td>
<td></td>
</tr>
</tbody>
</table>

#### 367 services of very different flavors
- iam
- rds
- dynamodb
- s3
- ...
- access-analyzer (permissions mgmt access level)
- cloud-search

© 2023 Andromeda Security
Permission Risk: 15,423 permissions to score

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Service</th>
<th>Criticality</th>
<th>Sensitive Info Exposure</th>
<th>Privilege Escalation Exposure</th>
<th>Resource Exposure</th>
<th>Deprecated</th>
</tr>
</thead>
<tbody>
<tr>
<td>List</td>
<td>iam</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tagging</td>
<td>glue</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read</td>
<td>s3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Write</td>
<td>cloud-srch</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permissions Mgmt</td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

https://github.com/ianne0036/iam-dataset
Policies: collections of permissions, applied to resources, in certain conditions
A set of non-trivial rules specifies permissions, resources, conditions

```
  "name": "AdministratorAccess",
  "document": {
    "Statement": [
      {
        "Action": [ "*" ],
        "Effect": "Allow",
        "Resource": "*"
      }
    ]
  },

  "name": "PowerUserAccess",
  "document": {
    "Statement": [
      {
        "Effect": "Allow",
        "NotAction": [ "iam:*", "organizations:*", "account:*" ],
        "Resource": "*"
      }
    ]
  },
Policy Risk: 1187 AWS Managed Policies + Custom Policies

**Policies:** collections of permissions, applied to resources, in certain conditions

A set of non-trivial rules specifies permissions, resources, conditions

---

**ReadOnlyAccess**

- redshift:DescribeEndpointAuth
- gamelift:GetComputeAuthToken
- waf:GetChangeToken
- sts:GetSessionToken
- snowball:GetJobUnlockCode
- lightsail:GetKeyPairs
- lightsail:GetBucketAccessKeys
- ecr-public:GetAuthorizationToken
  
  … (5026 permissions)

**ViewOnlyAccess**

- lightsail:GetKeyPair
- connect:ListSecurityKeys
  
  … (1191 permissions)

---

How do we aggregate the risk of individual permissions to create policy risk?
Policy Risk in Context: Specific Account and User

Users pose different risks:
What is the user’s role?
What is their status?

Risk of User in Account Across Policies

Account:
A policy that is exceedingly dangerous in production can be considered totally safe in a development account that lacks sensitive customer data

Policy Risk

Permission Risk
Policy Risk in Context: Specific Account and User

**AWS Account**
A cloud environment that contains data and resources

**Policy**
A set of Permissions (aka Actions) and the resources to which they apply
User/Identity Risk

• Types of users / identities in the system
  • Cloud admin
  • Cloud developer
  • Data scientist
  • Auditor
  • Contractor
  • Partner
  • Customer (authenticated vs. general webapp visitor)
  • IAM vs SSO user

• Human user attributes
  • Organizational role, usage pattern, peers, employment status, etc.

• Non-human identities
  • These identities run automated processes
  • Vital to business continuity
  • Unclear who owns the non-human identity, what if that user leaves?
  • Fear of disrupting a critical business operation
Account Risk

Security impact of account compromise:
- Customer Privacy
- Intellectual Property
- Business Continuity

Account risk metrics based on security impact:
- Does the account have sensitive data?
- What kinds of proprietary code are hosted there?
- What would happen if the account went down?

These factors should impact the access control decisions:
- Grant users read-only access or list-only?
- Control access to sensitive code and resources
- Who is allowed to create and alter infrastructure?
Account Risk Across All Users

How do we aggregate?
- Total risk of all users?
- Max risk across all users?
- A middle ground?

Risk of User in Account Across Policies

Policy Risk

Permission Risk

Other Aggregate Measures
- Risk of a user across all accounts
- Risk at whole cloud provider level
Once We’ve Modeled Risk, Then What?

Least Privilege

The goal of least privilege is to minimize impact in case of a compromise...

...by giving Kevin the right permissions to the right set of resources for the right reasons for the right duration at the right time...

...and do so without disrupting business agility
Our Approach at Andromeda Security

• Define risk and usage metrics to derive least privilege

• Automate decision making to ensure business agility

• Use Machine Learning to address scale and complexity
Thank you

Kevin Alejandro Roundy
Kevin@andromedasecurity.com