Security issues discussed in this talk are only for education purposes and to strengthen the research and intelligence efforts for enhancing the SECURITY and PRIVACY state of Development and Operations in the Cloud.

This talk does not relate to any of my previous or present employers.
- Aditya K Sood, PhD
- Cyber Security Advisor, Practitioner and Researcher
- Working in the security field for more than 11 years
- Regular speaker at industry leading security conferences
- Authored of “Targeted Cyber Attacks” Book
- Published Security papers in leading magazines and journals IEEE, ISACA,USENIX, and others.

- Web portal: [https://adityaksood.com](https://adityaksood.com)
Agenda

- A Look into the Cloud Market
- A Look into the Recent Security/Privacy Breaches in the Cloud
- Cloud Data Breaches: Top 7 Causes
- Exposure and Misconfigurations: Development and QA Systems
- Real World Case Study: Securities Lending Firm / Banks and Exposed Systems in the Cloud
- Introduction to SPADE
- Conclusion
- Q/As
Cloud Market: Why Do We Care?

### Table 1. Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)

<table>
<thead>
<tr>
<th>Service Type</th>
<th>2018</th>
<th>2019</th>
<th>2020</th>
<th>2021</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Business Process Services (BPaaS)</td>
<td>45.8</td>
<td>49.3</td>
<td>53.1</td>
<td>57.0</td>
<td>61.1</td>
</tr>
<tr>
<td>Cloud Application Infrastructure Services (PaaS)</td>
<td>15.6</td>
<td>19.0</td>
<td>23.0</td>
<td>27.5</td>
<td>31.8</td>
</tr>
<tr>
<td>Cloud Application Services (SaaS)</td>
<td>80.0</td>
<td>94.8</td>
<td>110.5</td>
<td>126.7</td>
<td>143.7</td>
</tr>
<tr>
<td>Cloud Management and Security Services</td>
<td>10.5</td>
<td>12.2</td>
<td>14.1</td>
<td>16.0</td>
<td>17.9</td>
</tr>
<tr>
<td>Cloud System Infrastructure Services (IaaS)</td>
<td>30.5</td>
<td>38.9</td>
<td>49.1</td>
<td>61.9</td>
<td>76.6</td>
</tr>
<tr>
<td><strong>Total Market</strong></td>
<td><strong>182.4</strong></td>
<td><strong>214.3</strong></td>
<td><strong>249.8</strong></td>
<td><strong>289.1</strong></td>
<td><strong>331.2</strong></td>
</tr>
</tbody>
</table>
Recent Security Breaches: The Cloud

Autoclerk Database Spills 179GB of Customer, US Government Data
An open Elasticsearch database exposed hundreds of thousands of hotel booking reservations, compromising data from full names to room numbers.

ElasticSearch server exposed the personal data of over 57 million US citizens
Leaky database taken offline, but not after leaking user details for nearly two weeks.

Imperva: Data Breach Caused by Cloud Misconfiguration

Adobe left 7.5 million Creative Cloud user records exposed online
Exposed data primarily includes emails, but not passwords or financial information.

A hacker gained access to 100 million Capital One credit card applications and accounts
## Cloud Data Breaches: TOP 7 Causes

<table>
<thead>
<tr>
<th>S.No</th>
<th>Potential Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Misconfigured and Exposed S3 Buckets</td>
</tr>
<tr>
<td>2</td>
<td>No MFA-Protected APIs Access</td>
</tr>
<tr>
<td>3</td>
<td>Cloud WAF Bypasses and Misconfigurations</td>
</tr>
<tr>
<td>4</td>
<td>Exposed Critical Servers on the Internet {ElasticSearch, etc}</td>
</tr>
<tr>
<td>5</td>
<td>Default Admin Accounts {Critical Assets: Databases, etc}</td>
</tr>
<tr>
<td>6</td>
<td>Unpatched Critical Assets : Unmanaged Vulnerabilities</td>
</tr>
<tr>
<td>7</td>
<td>Malicious Insider: Understanding of Internal Cloud Environment</td>
</tr>
</tbody>
</table>
One of the Stringent Reason of Security Breaches in the Cloud

Exposures and Misconfigurations
Security and Privacy: Development, QA and Automation
Development, QA and Automation - Systems Security

- Security issues
  - Exposed systems - Jenkins | Apache Archival | Hastebin for Code Sharing
  - Exposed Elastic Search, Reddis
  - Exposed DNS Artefacts
  - Sensitive information disclosed in automation scripts
    - AWS accounts credentials
    - Jenkins credentials
    - Test accounts - staging and testing
    - Information disclosure about the deployed instances
  - Automation scripts broadly shared
    - No access control lists
    - Same accounts are broadly used across and shared on the fly
  - Data leakage and associated structure of data storage
● Jenkins Anonymous Access
● Information Disclosure: Build History / Users / Credentials
Exposed Apache Archiva: Staging Repository

- Apache Archiva: Exposed Interface
- Information Disclosure: Code and Software Repos
Exposed Hastebin: Code Sharing

- Hastebin: Code Sharing
- Utilizing The Hastebin for Malicious Purposes
• Exposed Accounts and Credentials:
  ○ Automation
  ○ Test Suites
  ○ Performance

```xml
<suite name="Test Jersey">
  <parameter name="userName" />
  <parameter name="password" />
  <parameter name="environment" value="prod" />
  <parameter name="tenant:token" value="/"></parameter>

  <test name="Policy Tests">
    <classes>
      <class name=""></class>
    </classes>
  </test>
</suite>
```

```python
class RestClient(object):
    """ Implements all Rest methods """

    def __init__(self):
        self.retries = 5
        self.backoff_factor = 0.3
        self.status_force_list = (500, 502, 504)
        self.session = None
        self.headers = {
```
- ElasticSearch Interface: Exposed
- Surf through the Cluster to Analyze Data

150+ GB Data is Exposed on Misconfigured Host Deployed on AWS
ElasticSearch Interface: Exposed

Surf through the Cluster to Analyze Data

- Potentially a Monitoring/Telemetry Cluster

55+ GB Data is Exposed on Misconfigured Host Deployed on AWS
- Redis Exposed: Key-Value Pair
- Configuration Settings Dumped

---

```
# Server
redis_version:3.2.12
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:7897e7d0e13773f
redis_mode:standalone
os:Linux 4.14.128-112.105.amzn2.x86_64 x86_64
arch_bits:64
multiplexing_api:epoll
gcc_version:4.8.5
process_id:2357
run_id:b412e31517ca41f3b2f530ea66c8b2be087c1c4a
tcp_port:6379
uptime_in_seconds:10920828
uptime_in_days:115
hz:10
lru_clock:12438050
executable:/usr/bin/redis-server
config_file:/etc/redis.conf

# Clients
connected_clients:1
client_longest_output_list:0
client_biggest_input_buf:8
blocked_clients:0

# Stats
total_connections_received:1913
total_connections_issued:13562
instantaneous_ops_per_sec:0
total_net_input_bytes:31884866
instantaneous_input_kbps:0.00
instantaneous_output_kbps:0.00
rejected_connections:0
sync_full:0
sync_partial_ok:0
sync_partial_err:0
expired_keys:0
evicted_keys:0
keyspace_hits:1
keyspace_misses:2
pubsub_channels:0
pubsub_patterns:0
latest_fork_usec:135
migrate_cached_sockets:0

# Connected Clients
id:1
name:age="0" idlen="0" flags="N" db="0" sub="0" psub="0" multic=1 qbuf="0" qbuf-free="32768" dblen="0" all="0" one="0" e
ventions cmd=client
```
DNS Interface Exposed

- Revealing Extensive Info about the DNS Artefacts
QA Systems, Securities Lending Org and Banks

Understanding the Parameters

- Web server running specific service was exposed on the Internet due to mis-configuration
- No authentication controls were implemented on the listed APIs
- APIs could be queried over HTTP channel and not HTTPS
- On validating the data, some valid SSN entries including test data was found but it was not possible make judgement
- The APIs did disclose on the type of the information was stored in the database which in itself

The Issue was “Disclosed Responsibly” and now Fixed.
Real World Case Study

- These web servers were found to be running in unauthenticated manner.

- On accessing the HTTP service hosted on TCP port 9000/9001, we found that the web server returned a list of few APIs.

- At first, this look normal but on looking further, we noticed that the API URL contained “Equifax” as the resource.
One of the parameter reveals information as: "**callbackUrl** to the bank system"

**Overall Scenario:** Callback URLs were pointing to the bank systems
It is expected that securities lending firm Development, QA and Automation systems were exposed on the Internet. The systems disclose extensive information about the working details of credit verification process. Further, the indicators show the systems were associated with BANK <Undisclosed> as well.

Credit Bureau: <Undisclosed>
Securities Lending Firm: <Undisclosed>
Let's start with the first set of slides.

Security and Privacy Controls: Interrelated and Correlated
What Now?

SPADE: Security and Privacy Augmented DevOps for Enterprises
Introducing SPADE

SPADE framework enables to ease out the process of handling security and privacy issues at scale. The framework follows the approach of "Cure the Error at the Source (CES)" thereby negating the direct effects on the environment.
● Framework to defend against **Security and Privacy Intrusions** in Cloud (SPIC)

● **Security and Privacy needs to coexist** in an integrated manner

● Compliance or **attestations are not equipped enough to solve the ground problems**

● Achieving **Security and Privacy by Design** - Data Risk Assessment for Privacy and Security (DRAPS)

● Measuring the **performance of implemented Security and Privacy Controls**
Conclusion - The Basics!

SECURITY and PRIVACY should be Architected in PRE-DEVELOPMENT Design and INLINE-OPERATIONS and not the VICE-VERSA

MAKE THESE CONTROLS CONTINUOUS AND NOT AS WHEN NEEDED!
Questions and Queries

- Thanks
- Twitter: @AdityaKSood
- Linkedin: https://www.linkedin.com/in/adityaks