ADDIS ABABA SCIENCE AND TECHNOLOGY UNIVERSITY
UNIVERSITY FOR INDUSTRY

Addis Ababa Science and Technology University

College of Engineering

DEPARTMENT OF SOFTWARE ENGINEERING

COmputer System Security

Individual Assignment

NAME : - ANTENEH GETNET

ID NO. :- ETS0200/14

SUBMITTED TO : Mr. Getnet

SUBMISSION DATE : Oct 28, 2025

1. Introduction

In the era of digital transformation, information security has become one of the most crucial aspects of modern computing systems. The increasing reliance on cloud services, online banking, and digital data storage has created immense opportunities for growth but has also exposed organizations to growing cybersecurity threats. The purpose of this report is to study one of the most notorious security incidents in the financial sector — **the Capital One Data Breach of 2019** — and analyze how a single configuration mistake led to the exposure of millions of customers' private data.

The report explores the background of the attack, the vulnerabilities exploited, the techniques used by the attacker, and the resulting impact on the **Confidentiality, Integrity, and Availability (CIA Triad)** of the system. Understanding this breach is significant because it highlights how even large institutions with strong security budgets can fall victim to human error and misconfiguration.

Furthermore, the report discusses the broader **cyber threat landscape**, explores **preventive countermeasures**, and provides **recommendations** for avoiding similar incidents in the future. By examining the Capital One breach in depth, we gain a realistic view of how information security failures occur in practice and how they can be prevented through proper planning, monitoring, and awareness.

2. Selected Attack: The Capital One Data Breach (2019)

The **Capital One data breach** occurred in **March 2019** but was discovered four months later, in **July 2019**, when a security researcher found confidential data posted online. The incident affected approximately **106 million individuals** — 100 million in the United States and 6 million in Canada.

The attacker, **Paige A. Thompson**, was a former software engineer who had previously worked for **Amazon Web Services (AWS)** — the same cloud service used by Capital One. Using her knowledge of AWS systems, she exploited a **misconfigured Web Application Firewall (WAF)** to gain unauthorized access to Capital One's cloud infrastructure.

Once inside, she was able to execute a **Server-Side Request Forgery (SSRF)** attack, which allowed her to retrieve credentials and access **Amazon S3 storage buckets** containing sensitive customer data. The stolen information included:

- Full names, birthdates, addresses, phone numbers, and email addresses
- Credit scores, credit limits, and balances
- Transaction histories and fragments of Social Security Numbers (SSNs)

- Bank account numbers for secured credit card applicants

This attack is particularly significant because it targeted a major **financial institution** that had invested heavily in cybersecurity. It demonstrated that **cloud misconfiguration**, rather than hacking into cloud systems themselves, can be a major security weakness.

The breach cost Capital One more than **$190 million** in legal settlements, customer notifications, and security improvements. Beyond the financial losses, the company suffered severe reputational damage and regulatory scrutiny from U.S. authorities.

3. Cyber Threat Landscape

The Capital One breach occurred within a rapidly evolving **cyber threat landscape**, where attackers constantly exploit vulnerabilities across digital ecosystems. Understanding this broader context helps explain how such an attack could happen and why it matters.

Types of Cyber Threats

1. **Malware:** Software designed to damage, disrupt, or gain unauthorized access to systems. Examples include ransomware, trojans, and viruses.

2. **Social Engineering:** Deceiving individuals into revealing confidential information through phishing emails, fake login pages, or impersonation.

3. **Insider Threats:** Attacks carried out by current or former employees who misuse their access privileges — as seen in Capital One, where the attacker had insider knowledge of AWS systems.

4. **Advanced Persistent Threats (APTs):** Long-term targeted cyber campaigns often used for espionage or political purposes.

5. **Cloud-based Attacks:** Exploiting misconfigured or weakly secured cloud infrastructure, as seen in this case.

Motivations of Cyberattackers

Attackers are motivated by different factors:

- **Financial gain** (e.g., ransomware or data theft for sale)
- **Espionage** (stealing secrets for competitive or political advantage)
- **Revenge or Activism** (hacktivists exposing companies for ideological reasons)
- **Curiosity or Ego** (demonstrating technical skills or gaining recognition)

In the Capital One case, Paige Thompson's motive appeared to be a mix of **ego and curiosity** rather than profit. She later boasted about her access on online forums, which eventually led to her arrest.

Real-World Examples

- **Equifax Breach (2017):** 147 million people affected due to unpatched software vulnerability.
- **Yahoo Breach (2013–2014):** 3 billion user accounts compromised.
- **Sony Pictures Hack (2014):** Carried out allegedly by North Korean actors for political reasons.

These incidents demonstrate the diverse nature of cyber threats and how critical it is for organizations to maintain strong, proactive defense strategies.

4. Vulnerabilities Exploited by Attackers

The Capital One attack was not caused by sophisticated malware but rather by **human error** and **misconfiguration** of cloud resources — one of the most common security issues today.

Key Vulnerabilities:

1. **Misconfigured Web Application Firewall (WAF):**
   The WAF was designed to filter malicious requests but was incorrectly configured, allowing the attacker to perform **Server-Side Request Forgery (SSRF)**.

2. **Over-Privileged Access Rights:**
   The WAF instance had permissions to access sensitive files in Amazon S3, which it didn't need.

3. **Unsecured Cloud Metadata Service:**
   AWS's metadata service provided credentials that the attacker could use once she exploited the SSRF vulnerability.

4. **Lack of Monitoring:**
   Capital One lacked real-time monitoring that could have detected the unusual access pattern earlier.

5. **Human Error and Negligence:**
   The configuration error went unnoticed during internal audits and vulnerability assessments.

These weaknesses underline how cloud systems, though reliable, still require **constant configuration management, logging, and security reviews**. Even a small oversight can expose millions of users.

5. Countermeasures for Risk Mitigation

To prevent similar attacks, organizations must adopt a **defense-in-depth** strategy — applying multiple layers of protection rather than relying on a single security mechanism.

Recommended Countermeasures:

1. **Regular Security Audits:**
   Conduct continuous configuration reviews and penetration testing on cloud environments.

2. **Access Control and Least Privilege:**
   Limit access rights to the minimum necessary. System components should not have permissions beyond their purpose.

3. **Data Encryption:**
   Encrypt data both at rest and in transit to protect it even if accessed unlawfully.

4. **Security Monitoring and Logging:**
   Use automated systems like AWS CloudTrail to track access and detect anomalies.

5. **Employee Training:**
   Human error remains one of the biggest risks. Continuous awareness programs can prevent simple mistakes.

6. **Defense-in-Depth:**
   Combine multiple layers of defense such as firewalls, intrusion detection systems, multi-factor authentication, and strong password policies.

7. **Patch Management:**
   Regularly update all systems to fix security vulnerabilities before they are exploited.

Implementing these countermeasures ensures that even if one defense fails, others remain in place to prevent or minimize damage.

6. Research and Analysis of the Attack (CIA Triad)

The **CIA Triad** — Confidentiality, Integrity, and Availability — provides the framework for understanding the full impact of this attack.

- **Confidentiality:**
  The attack gravely violated confidentiality. Sensitive personal and financial data of over 100 million users were accessed without authorization. Such breaches can lead to identity theft, fraud, and reputational loss for victims.

- **Integrity:**
  There was no confirmed manipulation or alteration of data. However, the fact that data could be copied or viewed without authorization undermines confidence in the integrity of the system.

- **Availability:**
  The breach did not cause significant downtime or service interruption, but system access was temporarily restricted during the investigation.

Overall, this incident shows that even when integrity and availability remain intact, a loss of confidentiality alone can have devastating effects on public trust and organizational reputation.

7. Technical Details of the Attack

The technical execution of the attack followed these main steps:

1. **Reconnaissance:**
   Thompson scanned for misconfigured servers on AWS that responded abnormally to HTTP requests.

2. **Exploitation:**
   She discovered that Capital One's Web Application Firewall (WAF) accepted arbitrary requests and was vulnerable to **Server-Side Request Forgery (SSRF)**.

3. **Accessing Credentials:**
   Using the SSRF flaw, she tricked the server into retrieving temporary credentials from the AWS metadata service.

4. **Privilege Escalation:**
   These credentials provided permission to list and download files from Capital One's S3 storage buckets.

5. **Data Exfiltration:**
   The attacker downloaded gigabytes of sensitive data and stored it locally.

6. **Disclosure:**
   She later shared the stolen data publicly on GitHub, where it was discovered by an ethical hacker who alerted Capital One.

This process highlights how simple misconfigurations can be chained together into a devastating breach.

8. Attack Mitigation and Prevention

If Capital One had implemented the following measures, the breach could have been prevented:

- **Proper Firewall Configuration:** Ensuring the WAF could not be exploited via SSRF.

- **Restricting Access to Metadata Services:** AWS now recommends using *IMDSv2* to prevent this kind of attack.

- **Continuous Monitoring and Alerts:** Automated anomaly detection would have flagged unusual access requests.

- **Zero-Trust Security Model:** No component or user should be trusted by default, even within the internal network.

- **Regular Penetration Testing:** Security experts can simulate attacks to identify hidden vulnerabilities.

The lessons from this breach reshaped many organizations' cloud security policies worldwide.

9. Incident Response Efforts

After being alerted in **July 2019**, Capital One immediately initiated an **incident response plan**:

- They **informed law enforcement** and collaborated with the **FBI**, leading to the attacker's arrest within two weeks.

- The company **publicly disclosed the breach** on July 29, 2019, demonstrating transparency.

- Affected customers were notified and offered **free credit monitoring**.

- Capital One worked with AWS and cybersecurity experts to **review all configurations** and **strengthen firewalls**.

Despite these efforts, the company faced lawsuits, regulatory fines, and the loss of customer trust. The incident response, though quick after discovery, was reactive — showing the importance of proactive monitoring.

10. Reporting and Recommendations

Based on this study, the following recommendations are made:

- Adopt a **Zero-Trust Architecture** across all systems.

- Conduct **quarterly cloud security reviews**.

- Implement **automated configuration validation** tools such as AWS Config.

- Enforce **multi-factor authentication** for all administrative access.
- Maintain **transparent post-incident communication** with customers.

These recommendations would enhance data **Confidentiality**, **Integrity**, and **Availability**, reducing future risks.

11. Discussion and Reflection

Analyzing the Capital One breach reveals that **most modern attacks exploit mismanagement rather than system design flaws**. It reflects how crucial continuous training, cloud expertise, and internal auditing are in preventing security lapses.

The case also emphasizes that **cybersecurity is not a one-time setup** — it is an ongoing process requiring vigilance and adaptation. A balanced focus on the CIA Triad ensures that even if attackers succeed in breaching one aspect, the overall system remains resilient.

12. Conclusion

The 2019 Capital One Data Breach stands as one of the most instructive cases in cloud security. It was not caused by advanced hacking but by a **simple configuration mistake**, showing how small errors can lead to large-scale disasters.

The attack compromised **confidentiality**, tested **integrity**, and prompted significant organizational changes in **availability management**. It has since become a global lesson for companies using cloud services: **security responsibility is shared** — between the cloud provider and the customer.

In conclusion, the Capital One breach highlights the urgent need for **strong configuration management, continuous monitoring, encryption, and human awareness**. As technology continues to evolve, the only sustainable defense is **constant adaptation and education**.

References

1. Capital One Financial Corporation. (2019). *Capital One Announces Data Security Incident*.

2. U.S. Department of Justice. (2019). *Former Seattle Tech Worker Arrested for Data Theft Involving Capital One*.

3. Amazon Web Services. (2019). *Best Practices for Security in the AWS Cloud*.

4. Krebs, B. (2019). *What We Can Learn from the Capital One Data Breach*.

5. Wired Magazine. (2019). *The Capital One Hacker Got Caught Because of a Basic Mistake*.

6. NIST. (2020). *Guide to Cloud Security Best Practices (SP 800-210)*.