CAPITAL ONE BREACH (2019)

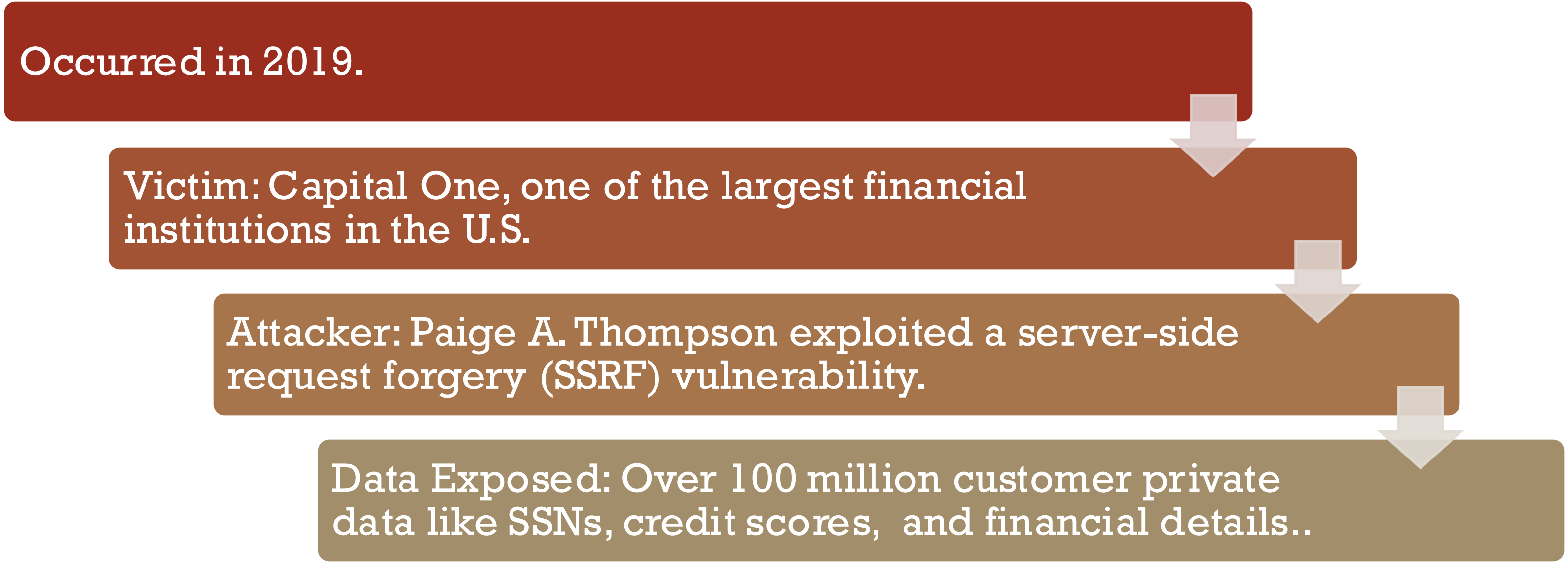
COSC 4362 Group 5

- Sandhya Malla

PROJECT OBJECTIVES

- ANALYZE THE CAPITAL ONE DATA BREACH.
- UNDERSTAND VULNERABILITIES IN CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (CIA)
- PROPOSE SECURITY MEASURES TO MITIGATE FUTURE RISKS.
- DEVELOP AN IMPLEMENTATION AND MONITORING PLAN.

BREACH OVERVIEW AND TIMELINE



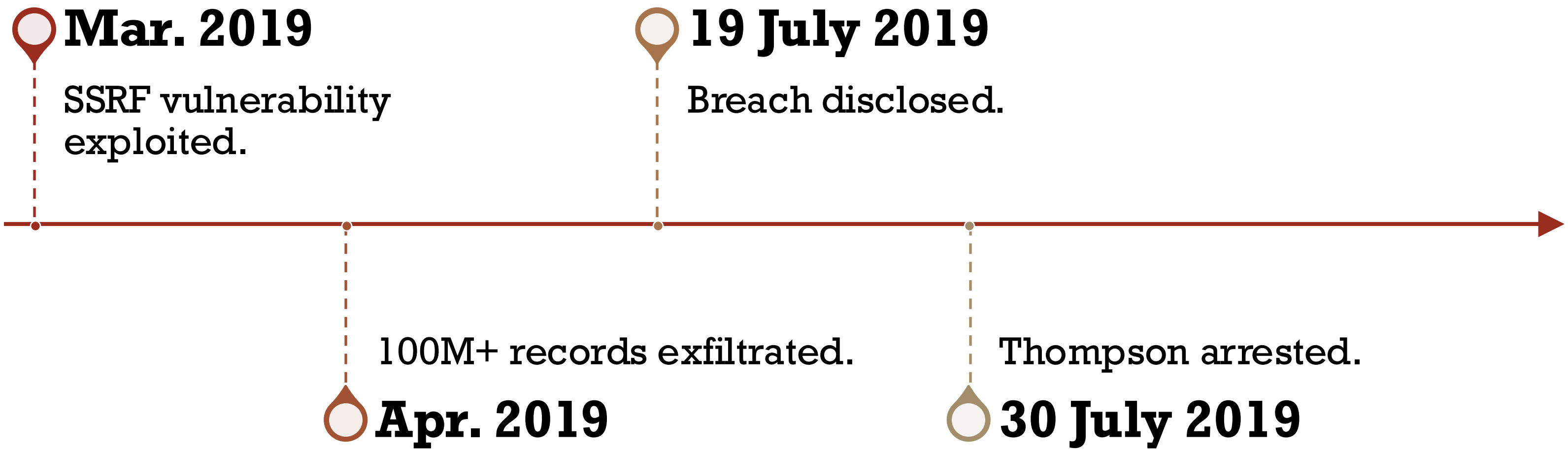
Occurred in 2019.

Victim: Capital One, one of the largest financial institutions in the U.S.

Attacker: Paige A. Thompson exploited a server-side request forgery (SSRF) vulnerability.

Data Exposed: Over 100 million customer private data like SSNs, credit scores, and financial details..

BREACH TIMELINE



Mar. 2019

SSRF vulnerability exploited.

Apr. 2019

100M+ records exfiltrated.

19 July 2019

Breach disclosed.

30 July 2019

Thompson arrested.

IMPACT ON CIA TRIAD

Confidentiality: Exposure of sensitive customer data (140K SSNs, financial details).

Integrity: No evidence of data tampering, but trust in systems weakened.

Availability: Services remained operational, but resources were diverted to damage control.

KEY FINDINGS AND SECURITY VIOLATIONS

Root Causes:

- Misconfigured Web Application Firewall (WAF).
- Lack of proactive vulnerability scanning and patching.
- Over reliance on default cloud settings.

Security Violations:

- Absence of Zero Trust Architecture.
- Weak access controls.

PROPOSED SECURITY MEASURES

Enhanced Encryption: AES-256 for data at rest, RSA-2048 for data in transit.

Improved Authentication: Multi-Factor Authentication (MFA).

Access Controls: Role-Based Access Control (RBAC).

Database Security: Data masking, regular backups.

Network Protection: Firewalls, IDS/IPS, and secure communication protocols (TLS 1.3).

IMPLEMENTATION PLAN

Top Priorities:

Encryption, MFA, RBAC.

Deployment Steps:

Secure sensitive data with AES-256 and RSA-2048.

Roll out MFA starting with high-risk users.

Configure RBAC based on roles and privileges.

Timeline:

Weeks 1–2: Encryption.

Weeks 3–4: MFA deployment.

Weeks 5–6: RBAC setup and audits.

MONITORING AND MAINTENANCE

Monitoring Tools:

- Security Information and Event Management (SIEM).
- Regular log reviews and anomaly detection.

Incident Reporting:

- Real-time alerts.
- Incident response protocols (categorize, escalate, document, review).

Continuous Improvement:

- Regular vulnerability scans and penetration tests.

COMPLIANCE AND TRAINING

Compliance:

Meet GLBA, PCI DSS, GDPR standards.

Vendor security audits.

Training:

Phishing awareness workshops.

Regular updates on security protocols.

Promote a security-conscious culture.

CONCLUSION AND LESSONS LEARNED

Key Takeaways:

- Misconfigurations can lead to significant breaches.
- Stronger encryption, MFA, and RBAC are critical to mitigating risks.
- Continuous monitoring and employee training are vital.

Future Focus: Proactive measures and adaptability in cybersecurity practices.