First American Financial Corporation Data Breach (May 2019)

NAME: HARUN TORLAK
COURSE: SECURE SOFTWARE SYSTEM DEVELOPMENT

Introduction

- **Overview:**
- In May 2019, First American Financial Corp. suffered a massive data exposure, leaking 885 million sensitive records related to real estate transactions.
- The breach was caused by an Insecure Direct Object Reference (IDOR) vulnerability, allowing unauthorized access to documents dating back to 2003.
- Significance: One of the largest financial data exposures in U.S. history, highlighting critical cybersecurity failures.
- **Why This Matters:**
- Real estate and financial institutions handle highly sensitive data (SSNs, bank details, mortgages).
- The breach exposed systemic security weaknesses in legacy systems and poor vulnerability management.

Background on First American Financial Corporation

- **Company Overview:**
- Founded in 1889, headquartered in Santa Ana, California.
- One of the largest title insurance and settlement service providers in the U.S.
- Handles mortgage documents, property deeds, and financial records for homebuyers and lenders.
- **Why Data Security is Critical:**
- Regulatory Requirements: Must comply with GLBA, NYDFS Cybersecurity Regulation, and state privacy laws.
- Trust Factor: Clients expect confidentiality for sensitive financial data.
- Financial Risk: A breach can lead to lawsuits, fines, and reputational harm.

Discovery of the Breach

- **Timeline:**
- May 24, 2019: Cybersecurity journalist Brian Krebs exposes the flaw.
- Vulnerability existed for years but was only discovered after public reporting.
- **Technical Cause:**
- **Insecure Direct Object Reference (IDOR) Flaw**:
  - No authentication required to access documents.
  - Sequential document IDs in URLs (e.g., https://firstam.com/doc=500 → doc=501 exposed another file).
  - No rate limiting or access logs to detect suspicious activity.
- **Types of Exposed Data:**
- **Personally Identifiable Information (PII):** SSNs, driver's licenses, passports.
- **Financial Data:** Bank statements, wire transfers, mortgage agreements.
- **Property Records:** Deeds, tax documents, purchase agreements.

How the Breach Happened

- **Root Causes:**

1. **Poor Software Development Practices:**
    - Lack of input validation and access controls.
    - Failure to implement OWASP Top 10 security principles.
2. **Legacy Systems:**
    - Old web applications with outdated security measures.
3. **Negligence:**
    - Internal security team knew about the flaw in December 2018 but failed to patch it.

- **Attack Scenario:**

- Step 1: Attacker finds an exposed document link.
- Step 2: Modifies the URL to access other files (e.g., incrementing document ID).
- Step 3: Scrapes millions of records undetected.

Company Response & Fallout

- **Immediate Actions:**
- Took the vulnerable portal offline within hours of Krebs' report.
- Hired forensic investigators (likely Mandiant or similar).
- **Legal & Regulatory Consequences:**
- $1 million settlement with NYDFS (2021) for negligence.
- Class-action lawsuits alleging violations of:
  - Gramm-Leach-Bliley Act (GLBA)
  - New York's Cybersecurity Regulation (23 NYCRR 500)
- SEC investigation into disclosure practices.
- **Reputation Damage:**
- Stock price dropped 3% post-breach.
- Loss of customer trust in real estate transactions.

Industry Impact & Regulatory Changes

- **Broader Implications:**
  - Increased scrutiny on title insurance companies' cybersecurity.
  - NYDFS Cybersecurity Regulation enforcement strengthened.
  - Shift in compliance: More firms adopted penetration testing and bug bounty programs.
- **Key Takeaways for Financial Firms:**
  - Proactive vulnerability management is critical.
  - Third-party audits can prevent such exposures.

Lessons Learned & Prevention

- **Security Best Practices:**
  Secure Coding: Train developers on OWASP Top 10 (especially IDOR).
  Regular Penetration Testing: Simulate attacks to find flaws.
  Access Controls: Enforce role-based authentication and multi-factor authentication (MFA).
  Monitoring & Logging: Detect unusual access patterns

Conclusion

- **Summary:**
- First American’s breach was preventable but resulted from negligence and poor security hygiene.
- Highlighted the real-world consequences of weak cybersecurity in financial services.
- **Call to Action:**
- **Businesses:** Invest in cybersecurity training and tools.
- **Individuals:** Monitor credit reports if affected by such breaches.

References:

- KrebsOnSecurity (2019) – Initial breach report.
- NYDFS Settlement Order (2021).
- OWASP IDOR Prevention Cheat Sheet.
- Wikipedia