Aadhaar Case Study

Unique Identification Authority of India(UIDAI)

By Suchit Reddi

Attack Category

(Software Vulnerabilities, Third Party Breach)

Description of the Attack Category to teach the reviewer about the attack

Third-Party Breach – The breach into the Aadhaar database was through a state-owned utility company named Indane, a gas company.

Software vulnerability – The main vulnerability which allowed access to the Aadhaar database was the insecure API used by Indane. The API had no access controls. It did not have any rate limit, allowing thousands of requests each minute from just one device.

Company Description

UIDAI(Unique Identification Authority of India) is a government body of the Indian Government established to issue Unique Identification Numbers (UID) named Aadhaar, to all residents of India, and is responsible for its enrolment, authentication, operation, management, and security.

Summary of the security incident and data breach

The largest ID database in the world, Aadhaar, was established by UIDAI in 2009. It contains information on 1.34 billion Indian citizens as of Oct 2021. When the breach occurred in 2018, there was information on 1.1 billion people in the database.

A state-owned third-party utility company named Indane used an API to retrieve data from the database. The API has no access controls, which gave anyone who hacked Indane access to the Aadhaar database. A security researcher, Karan Saini, discovered this weakness and notified them but was denied by the UIDAI. US tech portal ZDNet also contacted Indian authorities but was met with denial. It was not until March 23, 2018, after ZDNet published a story, that Indian authorities took the vulnerable access points offline.

The feeble security measures by UIDAI are likely to have catastrophic consequences. Virtually all Indian citizens registered for Aadhaar became potential victims of identity theft and other crimes stemming from it. Details like Name, Gender, Contact Information, Address, and Bank Account Details were available through the breach.

Global Risks Report 2019 of The World Economic Forum (WEF) acknowledged this as the most significant data breach until 2018.

Timeline

Aadhaar Attack

1. **UIDAI outsourced critical procedures like equipment manufacturing to private companies and gave access to important Personal Identifiable Information (PII) to third parties like Indane.**
2. UIDAI did not have good security practices and policies to secure the data of citizens. It did not monitor for vulnerabilities in its database and did not try to assess the risks from third parties.
3. Indane used an API endpoint with no access controls to retrieve data from the Aadhaar database of UIDAI. The endpoint was vulnerable to attacks. It did not have a rate limit, which allowed attackers to send thousands of requests.
4. The API's endpoint used hardcoded access token, which, when decoded translates to "INDAADHARSECURESTATUS", allowing anyone to query Aadhaar numbers against the database without any authentication.
5. Security researcher from New Delhi, Karan Saini, discovered the vulnerability, but UIDAI denied it.
6. WhatsApp groups gave out access to the Aadhaar database for a low price, and a few groups even distributed software to print their Aadhaar cards for as low as $10. There will be ongoing catastrophic consequences because of this attack, like identity theft etc.

Vulnerabilities

Overall Summary

UIDAI did not have third-party vetting; it did not assess the risks posed by allowing insecure third parties to access its data.

It was not ready to accept that it needed to improve its security just because it was a government body, even after being informed about the breach, which only increased the damage caused.

Insecure third-party access

UIDAI did not assess the security of its state-owned utility company – Indane. It resulted in a potential breach of details of 1.1 billion Indian citizens.

Lack of awareness

UIDAI did not have basic security measures in place and did not care to correct its mistakes even after being notified about the breach.

Weak access token

The hardcoded access token was very easy to decode and was "INDAADHAARSECURESTATUS", which was very straightforward.

Insecure API Endpoint

Indane's API endpoint did not have access controls. It did not have a rate limit. It resulted in attackers being able to send thousands of requests for data and extract large amounts of information.

Costs

- Personal Identifiable Information of 1.1 billion Indian citizens was potentially breached.
- There were no monetary losses directly on UIDAI just because it was a government body. It just denied the breach, and in turn, UIDAI filed a lawsuit against The Tribune, an Indian newspaper that reported about the breach.

Prevention

- The breach was caused mainly due to outsourcing sensitive work to private third parties and then neglecting the security measures taken by these third parties.
- The breach could have been prevented if UIDAI had corrected its mistakes when the breach was brought to its notice.