Incident Report

For the 2017-18 data breach on Aadhaar and the UIDAI

Contents

Executive Summary

Between 2017 and 2018, several lapses in security allowed for information within Aadhaar's databases to be compromised, which ultimately left upwards of 1.2 billion records exposed. The information within these records included names, addresses, emails, and Aadhaar card numbers.

2017 saw the start of a series of small data breaches caused by poor security on government websites. This list includes, but is not limited to websites for social assistance, payment reports, employment, and insurance. By using select government websites, it was easy for attackers to access the databases with no authentication. In some cases, the databases were easily accessible via Google.

At the start of 2018, individuals began selling access to the Aadhaar database for a relatively low price on WhatsApp. The software being sold also gave users the ability to create and print new Aadhaar cards. In addition to the software, people also sold individual records for a very low price, less than 10 cents in the US.

Executive Summary

In March 2018, a software patch was created and released which disabled key security features in the Aadhaar software including eye scanning and GPS tracking. This resulted in the entire Aadhaar database being exposed and easy to access. The software patch was assembled using code from older versions of the Aadhaar software and is easily installed by copying and pasting select files in the correct locations.

Given the nature of this software patch which deliberately makes changes in Aadhaar's code in order to disable security features, it is reasonable to assume this is the work of an insider threat. The person who made the software patch likely had a lot of knowledge of the systems which make Aadhaar function, which is only feasible by an insider.

Background

As of 2023, India has become the most populous country in the world. Such a large population also means a considerable portion of people living close to or below the poverty line. In the past, it has been difficult for people to get any resources from the government, often requiring complicated paperwork and many forms of identification. In order to streamline the process of getting these people the resources they need, and in general make easier the process of dispersing money to Indian residents, Aadhaar was created in 2009.

Aadhaar is a 12-digit unique identification number for Indian residents, similar to a social security number in the US. In the process of obtaining an Aadhaar card, residents need to provide a fingerprint and eye scan as well as photos of their face. However, the Aadhaar card is now used as an easier way of identifying someone. Ever since its creation in 2009, Aadhaar has become more than just an id and is also used as a driver's license, passport, and ATM card. Generally, Aadhaar aims to become the one card that people need.

Timeline

Overview

This section serves as a chronology of the events leading up to Aadhaar's data breach. Broadly speaking, based on the evidence provided, it is reasonable to assume the large quantity of exposed accounts and Aadhaar numbers are due to insider threats, while others are due to poor security on government websites.

May 2017: Government Website Leak

In May 2017, several government websites including those for social assistance, payment reports, employment, and insurance caused between 130-135 million Aadhaar numbers to be exposed.

August 2017: Website Leak #2

In August 2017, a Punjab government website exposed 20,100 Aadhaar numbers from applicants of a low-cost housing program.

Timeline

January 2018: Database Exposure

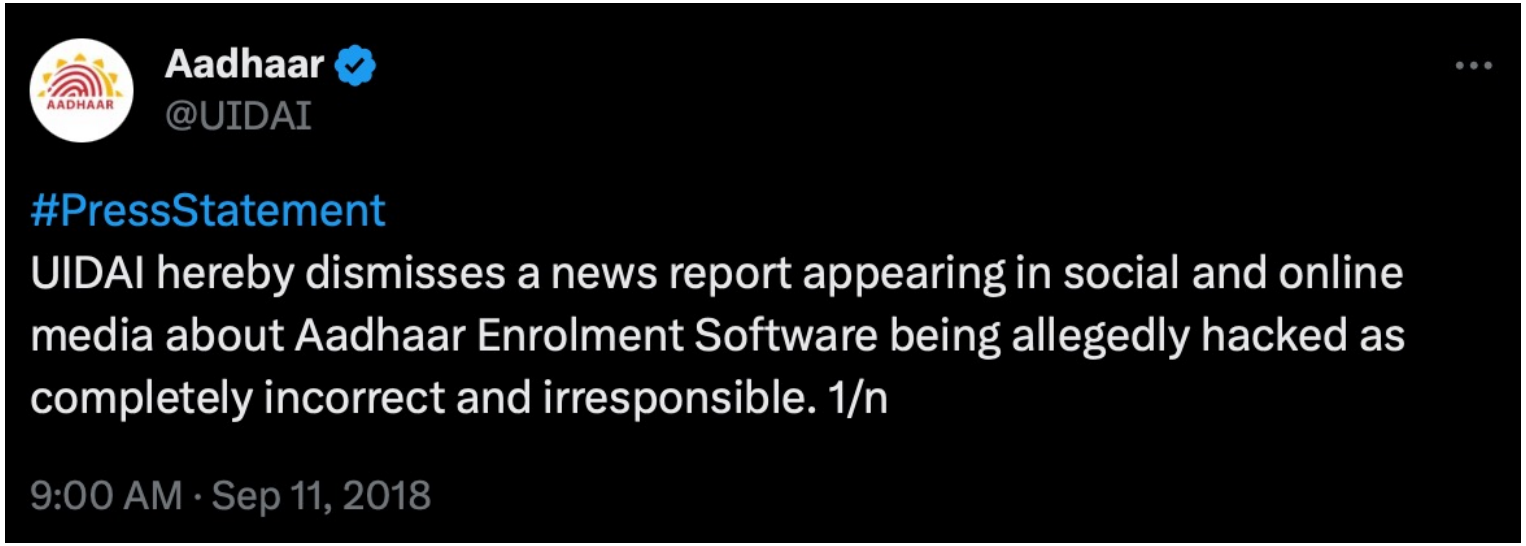
In January 2018, an individual on WhatsApp started offering access to the full Aadhaar database, containing personal information such as names, emails, and addresses, for around $8. Individual records could also be bought for less than 10 cents.

March 2018: Software Patch

In March 2018, a software patch was created which allowed users to bypass Aadhaar's security features such as iris scan and GPS location to allow access to the enrollment software and database. This software patch, which was available for purchase at $35, caused the entire database to be exposed, which was around 1.2 billion records.

Follow-Up

Aadhaar runs a database containing the information of over 1 billion people. Due to the large customer base, it is of utmost importance not to bring customers any fear. Outwardly, Aadhaar and the UIDAI have acted as confidently as possible regarding security, insisting that the information exposed is not severe and that any biometric data is safe. On Twitter (now X), Aadhaar has further denied any issues in order to calm any fears.



Follow-Up

Internally, Aadhaar has used the several data breaches and website leaks as a sign to improve security for the future. Aadhaar's security team has been severely limited to the point of not even having a Chief Information Security Officer (CISO). That leadership role is handled by the Information Security Division of the UIDAI. Additionally, the UIDAI aimed to hire 20 bug hunters that would work in spotting vulnerabilities to avoid future large data breaches.

Several issues sparked from government websites failing to encrypt Aadhaar databases and keeping them open for the public to easily find and access through search engines. After the data breach, several government websites were shut down to prevent further issues, and in some cases, prevent them from further being able to enroll new users to Aadhaar.

Lessons and Conclusion

Having exposed the information of over 1 billion people, it is safe to say that the Aadhaar data breach is one of the worst the world has seen. However, just like any data breach, there are lessons to be learned from it. The average attack is built from careful planning and deliberation to break what may seem like an unbreakable barrier between the attacker and the desired information. That is far from the case for Aadhaar.

In 2017 and 2018, Aadhaar served as an example of how not to handle a company's security. They left their databases on the open web for anyone to find, and when Aadhaar was attacked further with all of their information exposed, they refused to acknowledge any issues or take any of the blame, instead preferring to tell the public that everything was okay.

Aadhaar is a prime example of a company with the mindset that "infosec isn't sexy." However, it is also an example of why it is of utmost importance. Without good security, the information of an entire country could be put at risk, just like with Aadhaar.

For further information, refer to the following:

The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment
https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/

Aadhaar Data Breach — How Sensitive Data Of 1.3 Billion Indians Was Compromised
https://medium.com/@rithikvgopal/aadhaar-data-breach-how-sensitive-data-of-1-3-billion-indians-was-compromised-cb01d0c2d7d3

Indian state government leaks thousands of Aadhaar numbers
https://techcrunch.com/2019/01/31/aadhaar-data-leak/

Personal data of a billion Indians sold online for £6, report claims
https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar

Aadhaar: 'Leak' in world's biggest database worries Indians
https://www.bbc.com/news/world-asia-india-42575443

The Aadhaar card Act 2016 and its silent features
https://www.legalserviceindia.com/legal/article-10833-aadhaar-card-act.html

Mapping a Threat Model for the Aadhaar Ecosystem
https://thewire.in/economy/mapping-threat-model-aadhaar-ecosystem

The national security case against Aadhaar
https://www.orfonline.org/research/the-national-security-case-against-aadhaar/

India's state gas company leaks millions of Aadhaar numbers
https://techcrunch.com/2019/02/18/aadhaar-indane-leak/

Report on Data Security: Aadhaar Meltdown in India
https://bloom.co/blog/report-on-data-security-aadhaar-meltdown-in-india/

Aadhaar Truth: UIDAI Never Appointed a Chief Information Security Officer, Reveals RTI
https://www.moneylife.in/article/aadhaar-truth-uidai-never-appointed-a-chief-information-security-officer-reveals-rti/56267.html

UIDAI Annual Report 2018-19
https://uidai.gov.in/images/AADHAR_AR_2018_19_ENG_approved.pdf

UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm
https://www.huffpost.com/archive/in/entry/uidai-s-aadhaar-software-hacked-id-database-compromised-experts-confirm_in_5c128ddee4b0e15b460af020#

UIDAI launches program to identify, block vulnerabilities in Aadhaar biometric database
https://www.biometricupdate.com/202207/uidai-launches-program-to-identify-block-vulnerabilities-in-aadhaar-biometric-database

One of the Largest PII Database - Suffered...!!!
https://www.fncyber.com/web-of-trust-casestudies/one-of-the-largest-pii-database--suffered


WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON