Aadhaar: Hacking into a Nation

Deepanshu Utkarsh

December 2018

Abstract

Aadhaar is an ambitious project by the government of India to assign a unique identifier to all residents of the country. Hundreds of millions of previously invisible residents are finally receiving their first set of official documents and identification. However, the system is marred by multiple security vulnerabilities and data leaks. It is cheap and easy to create a fake identity or steal someone's identity. Rumors abound that the CIA and other state actors already have entire copies of residents' demographic, biometric and financial data. UIDAI, the administrator of the system, has denied all claims of data breaches and vulnerable software by the security community. In fact, researchers and journalists reporting on the mess are harassed, sued, and pressed with criminal charges. In this paper, we will briefly look at some vulnerabilities discovered in the UID system and how they may be exploited. We will also explore how residents can protect their data and how UIDAI can revamp Aadhaar's architecture and design to strengthen its security.

1 Introduction

Aadhaar is a $1.4 billion project by the Government of India with the mission of assigning a unique identity to each of India's residents, through the

Unique Identification Authority of India (UIDAI). This 12 digit unique identifier (henceforth, UID) is backed by the resident's demographic (name, address, contact information) and biometric (fingerprints, iris, face) data. The project has had a rough history, with concerns raised about its legal validity, integrity and the security of its very sensitive data. Despite being marred by multiple data leaks and breaches, the government has continued to push the project onto unknowing residents instead of scrapping it and protecting their information.

In fact, since 2014, the government slowly started requiring that a UID be annotated for hundreds of activities like availing welfare food benefits, filing income taxes, buying a mobile device and even enrolling in a school or college. This led to concerns being raised about the creation of a surveillance state based on tracking residents' activities by their UIDs.

2 To the Community

As of December 2018, 1.2 billion people have been issued UIDs. This means that the government of India has the demographic and biometric data of about 18% of the world's population. This data is a goldmine for corporations looking to tap into this emerging market, soon to become the world's 5th largest economy. As right-wing populism rises, democracies are being challenged and wars are starting to be fought in cyberspace; the government being in possession of this data represents a political nightmare. What if China and the CIA get their hands on this data? (They probably already have.) How much would Amazon bribe the government to participate in citizen tracking and target ads? How many political dissidents is the government tracking and denying services to? How many voter registrations did the government delete because they predicted these voters would not support them?

These are not hypothetical questions. They are based on incidents that

have actually occurred and left behind evidence, collected by numerous security researchers whose concerns have been disregarded by the government. Unless there is strong political will to fix – or ideally, scrap – Aadhaar, India's cybersecurity and its citizens' data is at risk of being used to cause harm. Or worse, sell ads.

3 Scope of UIDAI

Everyone legally residing in India for 6 months or more is eligible to receive a UID. Enrolment in the system is completely voluntary – at least on paper. However, a UID is practically mandatory to deal with the government in any official capacity, from birth to death. Receiving a child's birth certificate requires the parents' UIDs, while registering someone's death requires the deceased's UID or a notary certifying they did not have one.

The UIDAI collects all 10 of a person's fingerprints, a high resolution scan of both of their irises and a picture of their face. Demographic data collected include name, sex, address, phone number, email address, and curiously, parents' names.

However, this is not the only data associated with one's UID. Multiple government agencies are allowed to associate UIDs with the data they collect. For example, hospitals have medical records associated with UIDs, the income tax department and banks have financial data associated with UIDs, and even internet and phone service providers have account data linked to a UID, among many others.

A breach in any one of these data stores is – by design – a breach in all of these systems. A motivated attacker could easily use someone's UID and an exploit for one of its authentication mechanisms to gather all of the data associated with that UID.

4 Vulnerabilities in Authentication

4.1 Authentication as a UID holder

UIDAI supports multi-factor authentication for UIDs. The choice and number of factors to use is up to the client (which could be a bank, social security, etc). According to its API documentation, "demographic data, biometric data, PIN, OTP, possession of mobile, or combinations thereof" are available authentication factors.

However, this multi-factor authentication scheme means that the effort required to secure all combinations of all factors is immense. If an attacker gains access to demographic data like address and phone number from, for example, an ISP, then they have already breached the demographic factor. Intercepting SMS OTPs is trivial on 2G networks – used by most of rural India – and stealing someone's phone is also easy.

These vulnerabilities exist even before we start thinking about vulnerabilities in the different pieces of software that run and support the UID system.

A particularly vulnerable form of authentication is offline authentication. Since many remote areas of India do not have reliable internet or phone connectivity, someone's UID and demographic details can be verified using a copy UIDAI signed QR code. This QR code can be downloaded from the UIDAI website by anyone who is able to authenticate a UID online using the OTP or email factor. A client can then scan the resident's QR code and verify the signature against the UIDAI certificate.

However – and this is big – you cannot change your demographic details at will. Your personal QR code remains the same as long as the certificate UIDAI used to sign it doesn't expire. Unless you change your name, sex, date of birth or address, your identity is compromised and could be stolen. If an attacker gets their hands on your personal QR code, you are in trouble and your identity

has been stolen, with no clear way to restore its integrity.

4.2 Authentication vulnerabilities at the enrolment stage

Enrolling people into UID is a particularly sensitive part of the system. If an attacker manages to get a UID against fake data, they can use this fake identity for any of the services that use a UID for authentication. Therefore, it would make sense to protect this phase of the process with the highest levels of security best practices. However, multiple critical vulnerabilities exist within this process, one of which the author was able to exploit to generate a UID with fake data.

The software used to enroll a resident is a thick client. Instead of sending a packet of raw data to the enrollment server and letting it authenticate the enrollment, much of the processing, verification and authentication happens on the client side. For example, the software tries to verify that it is running on a registered computer, is being operated by a registered operator and has not been tampered with. However, since the client is a Java binary, it is vulnerable to simple reverse engineering based attacks. Malicious attackers and agents have already gained the ability to pretend to be an authorized operator, agency and location by simply bypassing the functions that perform these checks in the software. The author was able to use `fernflower` 'to decompile the Java binary and look at the source code to make inferences about various stages of the client-side verification process.

Unfortunately, server-side authentication of the client is minimal. An ID for a registered operator and the pre-shared secret passphrase are all that is needed to put fake but verifable UIDs into the database. These credentials and patched enrollment software that bypasses verification of these credentials is widely available for as little as $20 on the dark web as well as several WhatsApp

groups created by current and former operators.

5 Response by UIDAI

The UIDAI has continually denied that vulnerabilities exist and have been exploited in its system, despite overwhelming evidence to the contrary. The UIDAI's approach to handling data breaches has been to sweep it under the rug, deny all claims despite evidence, and prosecute security researchers and journalists who try to raise awareness about the issue.

The incompetency of the people in-charge became very visibly evident when the government of India, responding to a legislative challenge about privacy and security in the Supreme Court of India, said that residents' data is protected with 13 feet high walls and 200 security cameras at their data center in Manesar, India. No evidence or claims were presented about the security of the data from cyber threats.

As an aside, there were no claims or evidence presented that geographically diverse backups of the data exist. In the event of systemic failure at the lone data center, the entire country's business operations could be paralyzed.

6 Action Items

6.1 For the people

As with any other context in which personal data can be vulnerable, it is important to practice correct cyber hygiene when dealing with UID data. Ensuring that minimal copies of one's UID and associated data exists across data stores is paramount. Exercise restraint and question any authority which requires that a UID be authenticated. After recent legislative challenges, many agencies that required a UID for all transactions are disallowed from doing so. If possible,

try to perform transactions with various agencies without a UID being cited. The most vulnerable piece is the information dense QR code associated with the UID. Sharing this code with anyone – even accidentally or partially – can be very dangerous. A malicious attacker could simply take a picture of your QR code and recover much of your PII, that too signed by the UIDAI. These data can be used to carry out transactions on your behalf. If possible, do not let the QR code be generated at all.

6.2 For UIDAI

While UIDAI advertises its multi-factor authentication system as a counter to the one-size-fits-all identity verification regime, the fact is that many of these factors are compromised. Due to the nature of some of these factors (eg. fingerprints), a resident's records can be permanently compromised.

A complete revamp of the system and its architecture is needed. A multi-factor authentication scheme that does not rely on client-side verification must be put in place. Use of factors that are easily compromised or are irreplaceable (eg. fingerprints) must be stopped. Instead of QR codes for offline authentication, smart cards are a much better option and are much better understood, considering tens of billions of them are used around the world. If compromised, it is easy to deactivate a smart card and create a new one. They can also be used as a factor for online authentication, significantly strengthening the security of the system, since secrets are never transmitted on the network.

A political will to restore UIDAI's credibility by having an open system for responsible disclosure is also important. Instead of pressing charges against security researchers and journalists, the UIDAI should reward them through a bug bounty program.

Putting technically minded people in-charge who have more than just a ba-

sic understanding of cyber security is also important. Incorrect and irrelevant statements made by politicians and bureaucrats are laughable and further motivate attackers to exploit this vulnerable system. This would include organizing and maintaining a blue team to continually pentest the architecture and discover and fix flaws and weakness before malicious actors do.

7 Conclusion

The personal and biometric data of 1.2 billion people is at risk. Cyber policy paralysis and bureaucratic incompetency are to blame. Despite a growing technology industry, security researchers are being ignored and prosecuted for bringing to light critical vulnerabilities in software that is supposed to safeguard this data. Without an overwhelming revamp of the architecture and design of the UIDAI system, it will remain vulnerable to attacks and exploits. From state actors like the CIA or the Chinese, who want cyber-political hegemony, to low level businessmen trying to hide their under-the-table income, everyone has had a piece of the pie. And no one has stopped them.

8 References

1. Datta, Saikat. India's ambitious digital ID project faces new security nightmare. *Asia Times*. May 1, 2018. `http://www.atimes.com/article/indias-ambitious-digital-id-project-faces-new-security-nightmare/`

2. Khaira, Rachna; Sethi, Aman; Sathe, Gopal. UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm . *Huffington Post*. September 11, 2018. `http://www.atimes.com/article/indias-ambitious-digital-id-project-faces-new-security-nightmare/`

3. Deepalakshmi, K. The long list of Aadhaar-linked schemes. *The Hindu*. March 24, 2017. https://www.thehindu.com/news/national/the-long-list-of-aadhaar-linked-schemes/article17641068.ece

4. UIDAI. Aadhar Authentication API Documentation. February 2017. https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf

5. Parker, Ian. The I.D. Man: Can a software mogul's epic project help India's poor?. *The New Yorker*. October 3, 2011. https://www.newyorker.com/magazine/2011/10/03/the-i-d-man

6. Jain, Mayank. The Dangers Of Aadhaar-Based Payments That No One Is Talking About. *Bloomberg — Quint*. January 17, 2017. https://www.bloombergquint.com/business/the-dangers-of-aadhaar-based-payments-that-no-one-is-talking-about

7. Palo Alto Networks. WHAT IS A ZERO TRUST ARCHITECTURE? . https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

8. Thomas, Derick. What UIDAI doesn't tell you about offline use of Aadhaar for KYC . *Medium*. November 19, 2018. https://medium.com/karana/what-uidai-doesnt-tell-you-about-offline-use-of-aadhaar-cc4d249adf4e