UIDAI’S AADHAAR SOFTWARE HACKED, ID DATABASE COMPROMISED, EXPERTS CONFIRM

NEW DELHI—The authenticity of the data stored in India’s controversial Aadhaar identity database, which contains the biometrics and personal information of over 1 billion Indians, has been compromised by a software patch that disables critical security features of the software used to enrol new Aadhaar users, a three month-long investigation by *HuffPost India* reveals.

The patch—freely available for as little as Rs 2,500 (around $35) — allows unauthorised persons, based anywhere in the world, to generate Aadhaar numbers at will, and is still in widespread use.

This has significant implications for national security at a time when the Indian government has sought to make Aadhaar numbers the gold standard for citizen identification and mandatory for everything from using a mobile phone to accessing a bank account.

A patch is a bundle of code used to alter the functionality of a software programme. Companies often use patches for minor updates to existing programmes, but they can also be used for harm by introducing vulnerability—as in this case.

***HuffPost India* is in possession of the patch, and had it analysed by three internationally reputed experts, and two Indian analysts (one of whom sought anonymity as he works at a state-funded university), to find that:**

The patch lets a user bypass critical security features such as biometric authentication of enrolment operators to generate unauthorised Aadhaar numbers.

The patch disables the enrolment software’s in-built GPS security feature (used to identify the physical location of every enrolment centre), which means anyone anywhere in the world — say, Beijing, Karachi or Kabul — can use the software to enroll users.

The patch reduces the sensitivity of the enrolment software’s iris-recognition system, making it easier to spoof the software with a photograph of a registered operator, rather than requiring the operator to be present in person.

The experts consulted by *HuffPost India* said that the vulnerability is intrinsic to a technology choice made at the inception of the Aadhaar programme, which means that fixing it and other future threats would require altering Aadhaar’s fundamental structure.

“Whomever created the patch was highly motivated to compromise Aadhaar,” said Gustaf Björksten, Chief Technologist at Access Now, a global technology policy and advocacy group, and one of the experts who analysed the patch at *HuffPost India*‘s request.

“There are probably many individuals and entities, criminal, political, domestic and foreign, that would derive enough benefit from this compromise of Aadhaar to make the investment in creating the patch worthwhile,” Björksten said. “To have any hope of securing Aadhaar, the system design would have to be radically changed.”

Bengaluru-based cyber security analyst and software developer Anand Venkatanarayanan, who also analysed the software for *HuffPost India* and shared his findings with the NCIIPC government authority, said the patch was assembled by grafting code from older versions of the Aadhaar enrolment software—which had fewer security features— on to newer versions of the software.

NCIIPC, or National Critical Information Infrastructure Protection Centre, is the nodal agency responsible for Aadhaar security.

Venkatanarayanan findings were confirmed by Dan Wallach, Professor of Computer Science, and Electrical and Computer Engineering, at Rice University in Houston, Texas.

“Having looked at the patch code and the report presented by Anand, I feel pretty comfortable saying that the report is correct, and it could allow someone to circumvent security measures in the Aadhaar software, and create new entries. This is pretty feasible, and looks like something that would be possible to engineer,” Wallach said.

Indian authorities have declined comment, despite *HuffPost India* reaching out to both NCIIPC and the Unique Identification Authority of India (UIDAI) on more than one occasion since July this year.

While NCIIPC requested a copy of the patch, which *HuffPost India* provided in the same month, the agency has declined to share its findings. UIDAI did not respond to *HuffPost India*‘s mails.

A SERIES OF PRAGMATIC CHOICES

The genesis of the current hack lies in a decision, made in 2010, to let private agencies enroll users to the Aadhaar system in order to speed up enrolments. That year, Mindtree, a Bengaluru-based company, won a contract to develop an official, standardized enrolment software — called the Enrolment Client Multi-Platform (ECMP)— that would be installed onto the thousands of computers maintained by these private operators.

Apart from private enrolment agencies, the UIDAI also signed enrolment agreements with “common service centres” — village-level computer kiosks that help citizens access common e-governance services such as pensions, student scholarships etc. By February 2018, these centres were responsible for enrolling 180 million Indians.

This decision to install the software on each enrolment computer, said cyber security expert Björksten, "puts the running of critical components of Aadhaar in the hands of the enemies of the system".

A more secure choice would have been a web-based system in which all software would be installed on the UIDAI's own servers and enrolment operators would have a user name and password to access the system.

(A useful analogy is the difference between Microsoft Word — which is installed on computers — and web-based Google Docs, which is hosted online by Google, and users simply log on to use the service.)

B. Regunath, a software architect who led the team at Mindtree that worked on the project, said web-based enrolment software for Aadhaar was not practical at the time because many parts of the country had very poor Internet Connectivity.

"People were cranking up generators just to light up power and do the enrolment. How can they do an online upload of those packets?" asked Regunath, who has since moved to a senior technical position at Flipkart.

"We launched and issued the first Aadhaar card just three months after being selected," Regunath said, recalling that the launch was done urgently to meet a publicly announced deadline, without all the software features in place.

To compensate for handing effective control of the enrolment process to thousands of operators scattered across the country, Regunath's team added security features to the software — most prominently, a feature that required all operators to log in to the software by first providing their own fingerprint or iris scan. Any laptop being used had to first be registered with the UIDAI as well.

"We added a feature to check if the operator is certified, fixed people meddling with the system, we added a feature to check if the enrolment guys are running pirated or un-updated versions of Windows," Regunath said.

The UIDAI had also mandated that each computer used for enrolment was attached to a GPS device to ensure enrolment was done within the physical confines of the authorised centres.

Yet by early 2017, these carefully considered security features were bypassed by an elegant software hack that began circulating among the private enrolment operators empanelled to register a billion Indians to the Aadhaar database.

The use of this patch was so widespread that a YouTube search for "ecmp bypass" reveals hundreds of videos of private operators offering step-by-step guidance on how to subvert the UIDAI's security protocols.

"This is a straightforward, business-like, and utilitarian hack," said Björksten, the security analyst. "Having examined the entirety of the code, it is my opinion that the patch is the work of more than one coder."

Mindtree, the company that first developed the software, has acknowledged a list of queries sent by *HuffPost India*. The story will be updated once they respond.

INSTALLING THE AADHAAR HACK IS AS SIMPLE AS CUT AND PASTE

Sourcing the patch is as easy as gaining access to one of thousands of WhatsApp groups where the patch, and the usernames and passwords required to login to the UIDAI's enrolment gateway, are sold for as little as Rs 2,500.

Payments are made through mobile wallets linked to phone numbers that quickly go dead after the transactions are complete.

Using the patch is as simple as installing the enrolment software on a PC, and replacing a folder of Java libraries using the standard Control C, Control V cut-paste commands familiar to any computer user.

Once the patch is installed, enrolment operators no longer need to provide their fingerprint to use the enrolment software, the GPS is disabled, and the sensitivity of the iris scanner is reduced. This means that a single operator can log into multiple machines at the same time, reducing the cost per enrolment, and increasing their profits.

Bharat Bhushan Gupta, a 32-year-old former enrolment operator from Jalandhar, said operators like him were paid only Rs 30 per enrolment, so many operators began using the patch to make a little more money, charging between Rs 100 and Rs 500 in their own capacity. Gupta said he had not used the patch, and had written to the UIDAI CEO and others in the authority about its existence.

***HuffPost India* could not establish just how many enrolment centres used the patch, but even the UIDAI has admitted that the enrolment process has been marred by corruption. In 2017, the UIDAI said it had blacklisted 49,000 enrolment centres for various violations, and in February 2018, the UIDAI terminated all contracts with common service centres as well.**

Henceforth, only banks and government institutions like the postal service can enrol Aadhaar users. As a consequence, tens of thousands of young men, with rudimentary education but great familiarity with the Aadhaar system, were put out of work.

"We can't even make minimum wage," said Gupta, who used to run his own common service centre. "When they closed the enrolments, we had already formed WhatsApp groups through which we could help each other to use the software, and in these groups, there were some people who were offering new software that could be used to look up anyone's information."

In interviews, out-of-work operators claim they can still use the hacked enrolment software to generate enrolment ids (the first step in the Aadhaar registration process) and have tied up with sources working in authorised centres who complete the registration process for a fee.

WHO IS BEHIND THE AADHAAR HACK?

While the hack is being used by village-level computer operators, with no formal knowledge of programming, security researchers like Björksten and Venkatanarayanan say the hack represents a significant investment in time and resources — suggesting sophisticated well-trained adversaries.

"I get the sense that the patch does just the minimum needed," Björksten said. "The programmers have cut corners by utilizing previous versions of the Aadhaar code. This is a straightforward, business-like, and utilitarian hack."

"This patch has been created to be used, not just for the purpose of security research, or to highlight the security problems with the Aadhaar system." said Björksten.

"They have used some of the files from earlier versions of the Aadhaar software, which did not have these security features, and they have also made changes that remove other security checks," Venkatanarayanan said.

The changes are specific and targeted.

Apart from the changes mentioned previously, an analysis of the patch code by Björksten and Venkatanarayanan reveals one change that marginally reduces the fail-rate for iris recognition, resulting in more positive matches and making it possible to spoof the system with a high-resolution photograph.

Another change extends the duration of each login session — reducing how often a username and password needs to be entered, and thereby reducing security.

WHAT IS THE IMPACT OF THE AADHAAR HACK?

The software patch is unusual in that it doesn't seek to access information stored in the Aadhaar database, but rather looks to introduce information into it.

This, experts said, creates a whole new set of problems and could defeat many of Aadhaar's purported aims, such as reducing corruption, tracking black money, eliminating fraud and identity theft. It also means that the Aadhaar database is vulnerable to the same problems of ghost entries as any other government database.

"If anybody is able to create an entry in the Aadhaar database, then potentially the the person can create multiple Aadhaar cards. Then the same person can siphon off rations of multiple people," said Rajendran Narayanan, Assistant Professor, Azim Premji University, Bengaluru. "Since there are fixed quotas for rations, this would mean that several genuine beneficiaries would be excluded."

Similar problems can be introduced in all government schemes, Narayanan said.

There's a parallel between what's happening in India with what's happening in America," said Wallach of Rice University. "Not every American is born in a hospital, where a tonne of documentation is created automatically upon their birth. Many Americans, particularly poor Americans, give birth at home, where there's less documentation.

"This has recently become a problem for Americans born in the Rio Grande Valley, on the border between Texas and Mexico, where apparently some midwives were creating fraudulent documentation for non-Americans. The current response is an over-reaction to this, denying citizenship to rightful Americans in an attempt to remove an unknown number of frauds."

"The connection to India is pretty straightforward," he said. "India is trying to 'document' its citizens and they face a variation on the same problem as in America where many of the benefits of civil society are built on a bedrock of citizenship, but that citizenship itself can be a shaky foundation."

Ultimately, the very existence of the patch reveals that the Aadhaar framework, like any networked framework, is vulnerable, despite repeated assertions by UIDAI officials to the contrary.

This most recent vulnerability is an illustration of how extending Aadhaar to services and purposes it was never designed for has compromised the security of the entire project.

Anand Padmanabhan, a fellow at the Centre for Policy Research, said that from 2008 to 2011, Aadhaar shifted from being a purely government project to one that increasingly relied on participation by private players, without addressing the security implications of giving poorly supervised private individuals the capability to access the "end-point" — ie, the computers that connect to the UIDAI servers.

"Many cyber hacks happen on account of endpoint vulnerabilities," Padmanabhan said, "And by opening up the national identity database to private actors for easy on-boarding, the powers that be have exponentially heightened security threats."

The UIDAI has now responded, dismissing the report. You can read *HuffPost India's* rebuttal

(Downloaded from central employeesnews- 16-9-2018)