



Free Software Movement of India

www.fsmi.in

May 5, 18

To
Dr. AB Pandey,
CEO,
UIDAI.

Subject: Security of the Aadhaar personal data and ECMP Software

Dear Sir,

This is to bring to your attention a very serious issue which has come to our notice. There are WhatsApp messages circulating about a patched version of the Enrollment Client Management Platform (ECMP) software used for off-line Aadhaar enrollment, which can potentially be used to bypass geo-location and bio-metrics, and also change the mapping between personal data of Aadhaar holders and their bio-metric data.

There are also many videos (such as https://www.youtube.com/watch?v=i3ttp72P_Ww) uploaded to YouTube since middle of last year which claim to demonstrate how using a software patch to the ECMP software, geo-location and bio-metric security protection can be bypassed. According to these claims, the following can be done:

1. New Aadhaar enrollment can be made without any verification.
2. That personal information pertaining to existing Aadhaar numbers can be changed, bypassing any security checks including OTPs and bio-metric verification.

If this is true, then it is a matter of very serious concern as it endangers the sanctity of the entire Aadhaar database. We would like to know whether UIDAI authority has carried out any examination of these claims, and if there is any merit to these claims regarding the security of the Aadhaar enrollment software being compromised.

We would also like to bring to your notice that the PayTM account 7041704604 was mentioned in the youtube video https://www.youtube.com/watch?v=i3ttp72P_Ww. This account was tracked down to a certain Bharat B. who claimed to work for Computer Sciences Corporation (CSC) e-Governance division. Since CSC was contracted by UIDAI for Aadhaar Enrollment services, could this possibly be the case of rogue insiders who have used their access to this software to create illegal patched versions and are then selling it to the grey market?

Is UIDAI aware of this, as this has been reported in the press in the last few days? Please refer to:

1. <http://www.atimes.com/article/indias-ambitious-digital-id-project-faces-new-security-nightmare/>
2. https://www.buzzfeed.com/pranavdixit/for-30-anyone-can-add-or-edit-entries-in-indias-creepy?utm_term=.nggw1Jb2y#.ugaRJ9xNv
3. <https://medium.com/karana/aadhaar-a-self-certified-id-a63e299b36f5>

FSMI, Sy. No. 91, Beside AALIM, Green lands Colony, Gachibowli 'X' Roads, Sherilingampally, Hyderabad, Andhra Pradesh Ph: 040-20041263, +919490098011



Free Software Movement of India

www.fsmi.in

What are the steps the UIDAI is taking to make the Aadhaar system safe, as the security problems seem to emanate from inherent design flaws in the Client Server architecture of Aadhaar. Also, given that it appears that solicitations to sell the patched version of software seem to have been uploaded to the net, and doing the rounds of WhatsApp from at least the last one year, what is the sanctity of information stored in the Aadhaar database? What steps is UIDAI taking to verify the validity of data already uploaded by private players to the Aadhaar database? And whether it has been corrupted by such rogue patches being sold in the black market?

Given the seriousness of this issue and the imminent threat to our national security given the widespread use of Aadhaar for identification purposes, we hope that UIDAI would treat this matter with utmost seriousness. Hoping to get your quick response on this matter which concern all citizens of India. Continued silence by UIDAI on this issue is only fuelling speculations and rumours regarding what is supposed to be India's key data service.

Thanking You,
Yours Sincerely

Y. Kiran Chandra
General Secretary

Prabir Purkayastha
President