ORF ISSUE BRIEF
MAY 2017
ISSUE NO. 177

Privacy and Security Risks of Digital Payments

Bhairav Acharya

ABSTRACT Digital financial services have benefits but pose privacy risks that harm consumers, merchants, markets, and nations alike. Some payments systems in India suffer from vulnerabilities because they were not prospectively designed on the basis of the 'privacy by design' principle. At the back-end, the centralised storage of data is risky. At the front-end, faulty capture devices enable data misuse. Across the middle mile, data is transmitted without strong encryption. Payment systems must be redesigned to prospectively protect privacy and use unbreakable encryption and open standards. A data privacy legislation and a strong market regulator are also necessary.

INTRODUCTION

Digital financial services (DFS), like all data-driven digital services, offer consumers the opportunity to trade privacy for convenience. DFS promises financial inclusion for unbanked and under-banked populations in developing economies. Encouraged by the government and international actors, DFS is on the verge of rapid growth in India. However, without a strong data privacy and security regime, as is currently the case in India, DFS is risky and borderline exploitative.

To minimise fraud, biometrically-authenticated DFS is being heavily promoted in India. Biometric authentication might have advantages for consumers, merchants, service providers, and the market as a whole, but there are significant conceptual critiques of the use of biometrics for authentication.[1] In the absence of a data privacy and security regime, biometrically-authenticated DFS is even riskier than ordinary DFS. So far, the Indian government has failed to mitigate those risks through privacy and security measures.

To correct this dangerous imbalance in India's DFS sector, the country must take immediate steps to do the following: (i) disqualify all technologies that do not comply with the principle of 'privacy by design'; (ii) employ the highest standards of unbreakable encryption to secure data; (iii) mandate the use of open standards; (iv) enact an intelligent data privacy legislation that vests consumers with enforceable rights; and (v) create an independent, expertise-driven market regulator.

Biometrically-authenticated payments: How they work

The biometric properties of over 99 percent of adults in India are digitally stored in the national 'Aadhaar' database.[2] From a regulatory point of view, there are three parts to a biometrically-authenticated payments system. At the back-end, every consumer's Aadhaar data is linked with their bank account. At the front-end, the system manifests as a biometric-capture device—or, in the future, an app. Between the two ends, the system consists of a data transmission network.

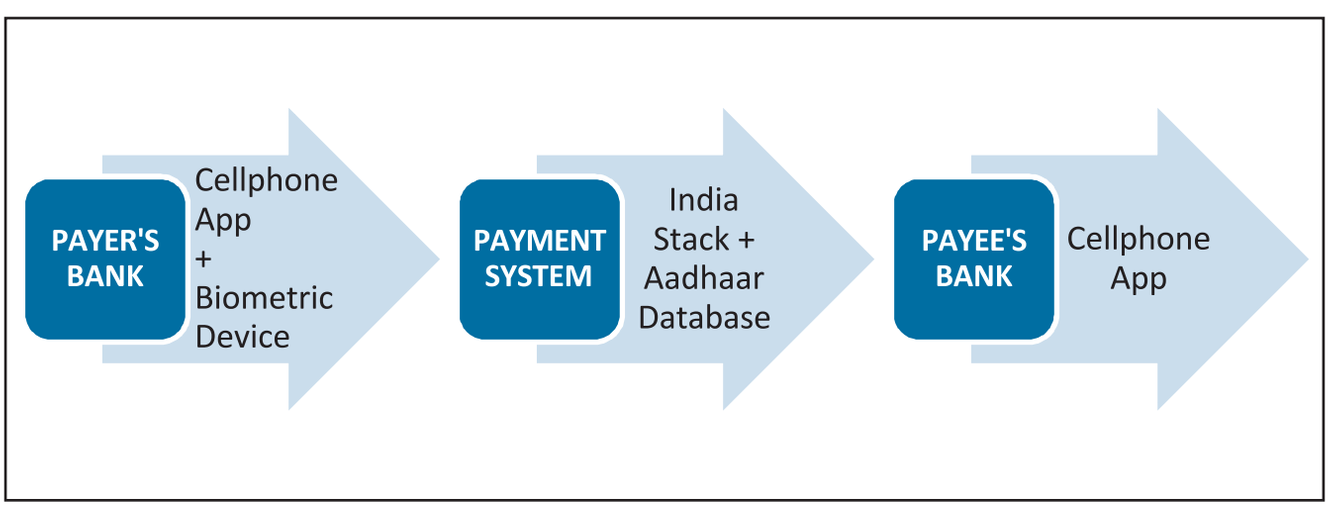
The Unified Payments Interface (UPI), a government-built payments system, already links consumers to banks on the basis of registered cellphone numbers and password authentication. The Aadhaar-Enabled Payments System (AEPS), which builds on the UPI's architecture, adds biometrics as another authentication measure. A consumer initiates a transaction by submitting her biometrics via a merchant's fingerprint reader, they are authenticated by reference to the database, and funds flow from that consumer's bank account. Commercial DFS providers who want to biometrically authenticate their users can build on top of the UPI's architecture.

The Aadhaar database is access-controlled, albeit imperfectly.[3] DFS providers cannot directly access biometric records at will. A set of computer codes known as the 'India Stack' enables third-party software to plug into the database. In the UPI's architecture, the India Stack is an intermediary that separates consumers and banks from the database. In the three-part regulatory model for digital payments described above, the India Stack lies between the front-end and middle mile.

PRIVACY AND SECURITY RISKS

All data-driven digital services, including DFS, pose privacy and security risks which arise from

Figure 1: How biometrically-authenticated digital payments take place



bad data practices. From a privacy perspective, bad practices include non-consensual or excessive data collection, sharing, storage, and use; unchecked data brokerage; and failure to de-identify data. From a security perspective, bad practices include the use of weak encryption, poor technical controls, poor cyber intelligence, and centralised data storage.

The negative impact of bad data practices affects consumers, merchants, and the market. Consumers are harmed by data breaches, identity theft, discrimination, reputational damage, and actual loss. Merchants are harmed by loss of goodwill, criminal liability, and actual losses arising from indemnities, damages, and penalties. The market is harmed by a loss of public confidence in digital services, cyber vigilantism, and the growth of informal mechanisms.

Countries themselves can be harmed by bad data security practices. For instance, hostile intrusions into payment systems that divert data flows can cause economic chaos, or large-scale breaches of biometric data can result in DFS being crippled by fraudulent transactions. The more data that a hostile actor can access, the greater the harm that can be caused. Indeed, cyber war doctrines are premised on the exploitation of an adversary's digital security weaknesses to cause economic damage.

SPECIFIC VULNERABILITIES

India's Aadhaar-Enabled Payments System, as well as the Unified Payments Interface, has specific privacy and security vulnerabilities based on the location of data in the system—at the back-end, middle mile, or front-end. Similar vulnerabilities are expected to emerge for any other future payments system built on the Aadhaar database.

At the back-end, Aadhaar data are stored in a central database. Centralising the storage of sensitive data is universally acknowledged as a bad security practice and there are enough examples of the risks involved. In June 2015, for instance, the United States Office of Personnel Management's servers—a central storage location for government data—was breached and the details of 21.5 million people, including the fingerprints of secret agents, were stolen.[4] Centralised databases are so-called 'honey pots' which incentivise hostile intrusions.[5]

At the front-end, user biometrics are captured by devices connected to several UPI-enabled apps developed by banks and the government. Commercial DFS providers that build on the UPI's architecture can develop their own apps. However, several existing capture devices create a cache for biometric images, which means that fingerprints are locally stored for future use.[6] In one instance in Delhi, 397 fraudulent transactions were made on the basis of a single fingerprint capture.[7]

After it is captured, biometric data travels in packets up and down the UPI's middle mile via the internet protocol. Internet data packets can be protected to various degrees—from totally unprotected to unbreakably encrypted. Consumers cannot choose their level of encryption, as they are reliant on the UPI to secure their data. The UPI's guidelines stipulate the use of unbreakable encryption to transmit passwords but not the biometric data itself.[8] If sensitive data is being transmitted in the clear, it becomes a serious vulnerability.

Because the UPI uses the internet protocol, there are more encryption options to secure the data. On the other hand, payment systems built on the USSD (unstructured supplementary service data) protocol, which is a voice-era cellular technology, are insecure by design.

USSD is notoriously hackable and its legacy security features are regarded as primitive in today's digital world. Thankfully, USSD payments never caught on in India and, as the Indian market anticipates an imminent data revolution, this protocol is expected to die soon.

Some mobile payment systems in other parts of the world are based on the SMS (short message service) protocol, which is also unsafe for DFS as SMS suffers from a lack of encryption and is therefore relatively easy to intercept.[9] Ironically, SMS is still the dominant mode of achieving two-factor authentication in mobile payment services. The world's leading cryptographers have been warning of the dangers of SMS-based authentication since 2005 but the DFS industry has not been listening.[10]

CONCLUSION

The existence of vulnerabilities is not a reason to abandon DFS, but it does call for immediate and continuous efforts to secure payment systems. The first step is a re-design of digital payment systems in light of the privacy by design principle, which calls for default high-privacy technologies, always-on privacy controls, and end-to-end security through unbreakable encryption. Planners should proactively design privacy-sensitive systems on the basis of open standards. For instance, fingerprint readers that cache data are, on the face of it, overly intrusive.

End-to-end security through unbreakable encryption and multiple-factor authentication should be incorporated into payment systems by default. Absolutely no payment transactions should take place on insecure communications protocols such as USSD and SMS. As long as DFS uses legacy technologies that are insecure, its claim to be a cutting-edge industry is questionable. Only internet-based data transfers that are unbreakably encrypted are secure. And only open cryptographic standards will allow consumers to satisfy themselves of their data security.

The success of digital payments rests on openness. The UPI provides an open interface for DFS providers to plug into. While that is a step in the right direction, the principle of openness calls for more. Open protocols should be used for data communications and open formats for storage. The sector should adopt open technological standards—and where that is impossible, reasonable and non-discriminatory licensing—to spur innovation and drive down costs. Open standards are particularly important for smartphone makers to avoid the patent thicket and bring low-cost devices into the hands of consumers.

Code is law, so most privacy and security risks in the DFS sector can be minimised by design and engineering.[11] However, privacy legislation is necessary to mandate privacy by design. The same legislation must create enforceable privacy rights for consumers. It is true that traditional consumer privacy law, which is built on the 'notice and consent' model, is failing. However, consent is not dead; it simply needs to be re-imagined. One way to achieve accountability for data practices is through use-based regulation[12] and mandatory harm warnings[13] based on contextual expectations of privacy.[14]

Finally, to shape the creation of a vibrant DFS sector focused on innovation and growth, and to protect the interests of consumers and the national economy, India needs a strong market regulator. In December 2016, the Ratan Watal committee proposed to hive off the payments regulatory board of the Reserve Bank of India into an independent body.[15] When it is created, the new regulator must have constant

access to data privacy and security expertise. Only when data is well regulated can DFS fulfill its potential for spurring rapid, transformational socio-economic change.

ABOUT THE AUTHOR

Bhairav Acharya is a Program Fellow at New America's Open Technology Institute in Washington DC. The views contained in this issue brief are personal.

ENDNOTES

1. Sunil Abraham, "It's the technology, stupid," *The Hindu Business Line*, March 31, 2017, http://www.thehindubusinessline.com/blink/cover/11-reasons-why-aadhaar-is-not-just-nonsmart-but-also-insecure/article9608225.ece.
2. Ravi Shankar Prasad, "UIDAI Achieves 111 Crore Mark on Aadhaar Generation Unique Identity Covers to Over 99 Percent Adult Residents of India," *Press Information Bureau* (Statement of the Minister of Information Technology and Law), January 27, 2017, http://pib.nic.in/newsite/PrintRelease.aspx?relid=157709.
3. Aman Sethi, Samarth Bansal and Saurav Roy, "Details of over a million Aadhaar numbers published on Jharkhand govt website," *Hindustan Times*, April 29, 2017, http://www.hindustantimes.com/india-news/in-massive-data-breach-over-a-million-aadhaar-numbers-published-on-jharkhand-govt-website/ story-EeFlScg5Dn5neLyBzrkw1I.html.
4. Brendan I. Koerner, "Inside the Cyberattack that Shocked the US Government," *Wired*, October 23, 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.
5. Sunil Abraham, interview by Sahil Makkar, "Aadhaar is actually surveillance tech," *Business Standard*, March 12, 2016, http://www.business-standard.com/article/opinion/aadhaar-is-actually-surveillance-tech-sunil-abraham-116031200790_1.html.
6. "Aadhaar Hacked," YouTube video, 1.46, posted by "Skoch Consultancy Services Pvt Ltd," May 3, 2017, https://www.youtube.com/watch?v=XrKwO2yW910.
7. Rajeev Deshpande and Mahendra Singh, "Probe against 3 firms for illegal use of Aadhaar biometrics," *The Times of India*, February 24, 2017, http://timesofindia.indiatimes.com/india/probe-against-3-firms-for-illegal-use-of-aadhaar-biometrics/articleshow/57321007.cms?from=mdr.
8. National Payments Corporation of India, "Unified Payments Interface: Procedural Guidelines" (Version 1.5, July 2016, page 5 of 62), http://www.npci.org.in/documents/UPI_Procedural_Guidelines.pdf.
9. Samuel Gibbs, "SS7 hack explained: what can you do about it?" *The Guardian*, April 19, 2016, https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls; Parmy Olson, "SIM Cards Have Finally Been Hacked, And The Flaw Could Affect Millions Of Phones," *Forbes*, July 21, 2013, https://www.forbes.com/sites/parmyolson/2013/07/21/sim-cards-have-finally-been-hacked-and-the-flaw-could-affect-millions-of-phones/#33b6181a17b8.
10. Bruce Schneier, "The Failure of Two-Factor Authentication," *Schneier on Security*, March 15, 2005, https://www.schneier.com/blog/archives/2005/03/the_failure_of.html.
11. Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).
12. Craig Mundie, "Privacy Pragmatism," *Foreign Affairs*, March/April 2014, https://www.foreignaffairs.com/articles/2014-02-12/privacy-pragmatism.

13. Melissa W. Bailey, "Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things," *Texas Law Review* 94 (2016): 1042-44.

14. Helen Nissenbaum, "A Contextual Approach to Privacy Online," *Daedalus* 140 (2011): 32-48.

15. Committee on Digital Payments, Ministry of Finance, Government of India, "Medium Term Recommendations to Strengthen Digital Payments Ecosystem," December 2016, http://finmin.nic.in/reports/watal_report271216.pdf.

ORF OBSERVER RESEARCH FOUNDATION

Ideas • Forums • Leadership • Impact

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-43520020, 30220020. Fax : +91-11-43520003, 23210773.
E-mail: contactus@orfonline.org
Website: www.orfonline.org