BATTLE BETWEEN BANKERS AND HACKERS

Deepali Arya
Assistant Professor,
Vaish Degree College, Rohtak

Priyanka
Student and Researcher, MBA

Abstract

In an October note, RBI deputy governor SS Mundra said one of the key targets by the attackers is the credential of the customers, as it provides the key to the treasure. "Recent experience shows involvement of organized gangs and nation-state actors having huge financial backing. On the other hand, the cost of orchestrating such attacks is coming down. There are several reports indicating availability of credentials of customers for sale in dark web, which is really scary. Authors have tried to highlights the issues pertaining to cyber crime with the increase of online banking.

Introduction

As the government presses ahead with cash to less cash to cashless economy, the success of the transition will depend on how the battle between bankers and hackers plays out. Bankers must upgrade and fortify their cyber defenses as hackers attempt to pinch funds from banks or steal credit/debit card details of retail customers daily. If suddenly the easiest way to buy anything from soft drinks to cars is to use the mobile wallet, a few click of the mouse are all that is required to rob a bank.

True, in a country with 98% cash in circulation, electronic payments replacing cash will not be easy and will take time. But since demonetization kicked off on November 8, digital payments have got a fillip. That has opened up more opportunities for cyber pickpockets to try and steal card details, PINs, mobile wallets and siphon off money.

"India has been at the lower end of frauds as volumes were low. Now, I suspect that will change as digital payments volumes surge," says R Venkatachalam, managing director. India & South Asia, FIS Global

Akhilesh Tuteja, partner and global head of cyber security, KPMG says if the benefits of digital payments are exponential, so are the risks

India's central banker itself flagged off concerns in this regard. In an October note, RBI deputy governor SS Mundra said one of the key targets by the attackers is the credential of the customers, as it provides the key to the treasure. "Recent experience shows involvement of organized gangs and nation-state actors having huge financial backing. On the other hand, the cost of orchestrating such attacks is coming down. There are several reports indicating availability of credentials of customers for sale in dark web, which is really scary.

The security threat notwithstanding, bankers prefer the shift to a digital payments system. A physical bank branch transaction is 50 times costlier than a digital transaction. And as volumes increase scale will ensure even lower costs of digital transactions. The government's push emanates from a desire to track the flow of money and check corruption and black money generation.

The downside of a digital economy is that millions can lose money in seconds. A single hack can ensure millions of accounts being compromised, as it happened in October when 3.2 million card details were stolen in a malware related security breach. These cards from customers of State Bank of India, HDFC Bank, ICICI Bank, Axis Bank and others were used at ATMs. The stolen debit cards were used in China. The heist is still under investigation, but is almost forgotten in the scramble for a digital payments future.

Digital Carrots

Indeed, one of primary concerns over the rush to a digital economy, besides the challenge of drawing in swathes of people who do not even have a bank account, is the threat of cyber attacks. The government for now seems to be more focused on the second problem — goading people to embrace digital payments. On November 15, it announced a scheme to encourage digital payments between Rs.50 and Rs.3, 000, offering around Rs.340 crore in cash awards for such transactions. The twin schemes, Ducky Grahak Yojana and Digi Dhan Vyaypari Yojana is launched on December 25 and run by the National Payments Corporation of India (NPCI) for 100 days. NPCI is the nodal agency controlling e-transactions like Universal Payment Interface (UPI), USSD, NEFT and RTGS.

Mobile wallets are already experiencing a tremendous growth in transactions. The user base of the Chinese Alibaba-funded Paytm has climbed from 100 million to 170 million in a month. Likewise, Sales of Point of Sales (PoS) machines have risen 200 times since November 8.

“India is on the fastest track when it comes to growth of digital channels use in financial services. The troika of Jan-Dhan, Aadhaar and mobile is one of the catalysts in making it happen,” says Rajashekara V Maiya, head, Finacle product strategy, Infosys.

The problem is hackers won't be far behind. According to the latest available data from RBI, 13,083 and 11,997 cases related to ATM, credit, debit card and net banking fraud were reported in 2014-15 and 2015-16 (up to December 2015). The October breach of 3.2 million cards was the single largest of its kind in India. Globally, Juniper Research says value of online fraud transactions is expected to reach $ 25.6 billion by 2020 up from §10.7 billion last year. “This means by end of the decade $4 in every $1,000 of online payments will be fraudulent” says Maiya. The 0.4% fraud transaction does not include money that could be stolen from comprom ised accounts.

Another study by Assocham-PwC notes a surge of about 350% in cybercrime cases registered under the IT Act, 2000 between 2011 and2014. Madhur Singhal, partner Bain & Company, says as it happens with other payments, there is a risk if user does not understand how' e-payments work. “Just liko losing a signed cheque leaf exposes a consumer to fraud, being negligent with passwords; card details could pose a risk in wallet or net banking transactions."

Types of Fraud

There are three kinds of risks unique to e-payments.

One device- related risk. If someone loses their mobile phone and there are no passwords protecting the phone or the app, money in an e-wallet could be compromised, or, leaving your accounts open when making payments from a public device.

Two, risk from rights access. Connecting the e-wallets or other fintech apps with other apps like social networks could pose a risk of data leakage or a consumer unknowingly sharing information that should have been kept private.

Three, negligence in sharing passwords or OTP (one time password) with others especially when using these modes publicly.

There are some other risks that are common to e-payments as well non electronic payments — for example, giving away your account details to a third party. Provided the consumer takes basic precautions, the benefit of electronic payments far exceeds the inconvenience and transaction costs one would have incurred in other forms of payment, especially when the payment ticket sizes are small.

Besides, downloading unverified apps and software can compromise security. Users should download apps with high rating. Banking portals can get compromised as well. Altaf Halde, managing director, Kaspersky Lab says, "HTTPs (the small's for secure) was always thought to be safe. But hackers can get here as well."

Problems can arise at both the bank and user end. "While banks have to regularly update software and fraud detection systems, users should be aware of basics like changing passwords frequently, using unique passwords for different accounts (instead of the same for net banking, Face book, Twitter)."

The problem could be the hardware as well. When you download a mobile banking app you don't know if it is using hardware security or not.

Credit cards, debit cards, mobile wallets, net banking fall in two distinct buckets. Credit, debit cards work under Payment Card Industry (PCI) standards, reviewed every year. PCI DSS (Data Security Standards) are **a** set of instructions to store, process and transmit plastic transactions with details about firewalls configuration, storing passwords, information of users and so on. "If PCI is not adhered to the card can be compromised," says Venkatachalam. Card companies like Visa, Mastercard, and Amex do this but banks want to control customer information and hence vulnerabilities can exist at their end. Net banking comes under electronic payment channels and the security protocols are released by Internet Engineers Task Force (IETF). When net banking started more than a decade back it worked with 40 kb encryption which went up to 64 kb and now 128 kb. "This is very good. But when you are dealing with variety of people with varying ability to transact digitally, the chance of a hacker getting the better of you increases," says Tuteja. Even if the network is robust (in India it is maintained by RBI with NPCI as nodal agency), the leaks could be at the banks end (software not updated) or the user end.

Systems managing the links from origin to settlement of a transaction are robust and secured, yet probability of fraud exists at every stage for example, buying a water bottle at a road side vendor via card or m-wallet, transmission of details to authenticate user to ok buy, completing the purchase with user getting a SMS or confirmation slip and reconciliation at the backend. A hacker could get at any of the five stages—origin, transmission, transaction, settlement and reconciliation.

Frauds Spike

ATM'/Net Banking Frauds"

2014-15	2015-16 (till Dec: 5)
13,083	**11,997**

*credit/debit cards, “transactions

(Source: RBI)

Spate of Attacks

- October 3.2 million card details were stolen in India. Matter still under investigation
- Vulnerabilities in the m-wallet app led to exploitation by attackers. The originator of the transfer could get the amount reversed back to him without corresponding debit in the recipient's account in a large number of transactions (amount involved was around Rs.12 crore). Bank was not performing any real time reconciliation and noticed it only when there was a spike in transactions.
- An e-payment validation website of a large bank was hacked. Bank unaware of the incident till it was notified by a law enforcement agency. There was a Facebook post by a person from a neighbouring country claiming responsibility for the operation.
- In November 2016 cyber criminals broke into UK's Tesco Bank's computers and made off with about $ 5 million from accounts of 9000 customers.
- On August 2, 2016, Bitfinex, a Hong Kong exchange for trading digital currencies, said some of its customer accounts were hacked and bit coins stolen. The value of the stolen bitcoins has been reported to be $65 million.
- In Feb 2016 Bangladesh Bank was the target and an attempt was made to steal $1 billion and ultimately the attackers successfully got away with S81 million.
- In Feb 2015 cyber criminals infiltrated 100 banks in 30 countries and siphoned off $1 billion.

Keeping Cyber Criminals At Bay

- Treat your Smartphone as a bank
- Use strong, unique passwords on every website
- Keep your operating systems, apps and antivirus up to date
- Enable two-factor authentication wherever available (particularly for email and financial sites)

- Type out the link in the address bar of web browser instead of clicking on links
- Avoid links or attachments sent from unidentified sources
- Click the lock in your browser to ensure your connection is secure and that you are connecting to the correct organizations
- Monitor your accounts for unauthorized transactions
- Avoid sending financial or personal information by email
- Avoid clicking links or entering personal information on pop-up windows

References

- Manisha M. More and Dr. K. M. Nalawade(2014) :Cyber Crimes and Attacks: The Current Scenario,1st National Conference organized by NESGOI, Pune.
- Susheel Chandra Bhatt and Durgesh Pant(2011): Study of Indian Banks Websites for Cyber Crime Safety Mechanism,(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.10, Jayshree Chavan(June 2013): Internet Banking- benefits and challenges In An Emerging Economy, International Journal of Research in Business Management (IJRBM) ,Vol. 1, Issue 1, 19-26.
- Rupinder Pal Kaur(Aug.2013)-Statistics of Cyber Crimes in India: An Overview, International Journal of Engineering and Computer Science ,Vol 2,Issue 8. More et al., International Journal of Advanced Research in Computer Science and Software Engineering 5(12), December- 2015, pp. 743-749 © 2015, IJARCSSE All Rights Reserved Page | 749
- National Crime Record Bureau: Cyber Crime Statistics In India 2014: http://ncrb.gov.in/pdf
- Computer Emergency Response Team(CERT):http://cert.India.com
- Cyber Crime complaints 2015:http://rbi.org.in/Press-release
- Kevin Peachey (27 March 2015) Online banking fraud 'up by 48%', BBC NEWS , Personal finance reporter From the section Business retrieved from: http://www.bbc.com/news/business-32083781.
- BS Reporter (Mumbai July 10, 2015 Last Updated at 00:41 IST)- Cyber frauds on rise with increase in digital banking: Assocham -PwC, Business Standard, retrieved from : http://www.businessstandard.com/article/finance/cyber-frauds-on-rise-with-increase-in-digital-banking-assocham-pwc- 115070901104_1.html.

- Purba Das (Jan 5,2015,03.48 PM)- cyber crimes to surge in India Likely to Touch 3 Lakh, Business Insider, Retrieved from:http://businessinsider.in/cyber-crimes-to-surge-in-India-Likely-to-touch.
- Karthik (January 5,2015),Cyber crime to Double in India by 2015: A Report , world post
- Cyber Crime: A Financial Sector View, Government and Public Sector, NASSCOM.
- Assocham India: Cyber crimes in India, study by 2015, The Associated Chambers of Commerce & Industry of India
- History of Banking: http://en.wikipedia.org.wiki/Banking_in_India.
- Cyber crime News: http://timesofindia.indiatimes.com/tech/tech-news/cybercrimes-up-across-IndiaMaharashtra-tops.
- Cyber Crime News:http://ibnlive.in.com/news/cyber-crimes-up-by-51-percent-india-Maharashtra-ap-Karnatakatop-list.
- Cyber crime News:http://www.computerweekly.com/news/2240215532.Financial-services-sector-attract-mostcyber-crime.