Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

CERT-In Advisory CIAD-2017-0013

Advisories for Mobile Payment Channels

Original Issue Date: February 16, 2017

Description

The drive for cashless economy has provided opportunities for various payment services providers including prepaid payment instrument (PPIs) service providers for exploring innovative modes of digital transactions. Based on smart phone based mobile applications various payment transactions services are being provided.

The service providers augment for various innovative and new technical tools for payment transactions which sometimes provide new avenues for the hackers and therefore bring new kind of threats into the eco system. The payment systems provided by the PPI needs to ensure various properties like confidentiality, mutual authentication, integrity, proper access control, authorisation and non-repudiation etc.

Threat vectors for PPI service providers

Vishing attacks

It is also called as voice based phising. Vishing is a fraud in which the customers are tricked into revealing their critical and sensitive personal financial information to unauthorised persons/entities through voice based technology. It does not always occur through internet media alone. The vishing attacks are also being carried out using various voice based channels like ISDN PRI (primary Rate Interface), Mobile PRI (Primary Rate Interface), VOIP, Landline or Mobile telephone etc.

With the introduction of Next Generation Networks (NGN) in telecom networks and Fourth Generation of mobile technology which support end to end IP based technology, the chance of VOIP based Vishing attack is higher. It requires less technology background.

For prevention of Vishing based attacks

- Prevention of voice based banking /financial transactions and wallet services in any format and creation of sufficient awareness in this front.
- Regular dos and don¿ts to the customers through all modes of communications.
- Sharing legitimate phone numbers of service providers needs to be shared constantly with the customer.
- Educating customers suitably while receiving calls asking for sensitive information.

Phishing attacks

The hackers may try to clone/copy/spoof the legitimate mobile applications with high accuracy. This creates the risk of phishing attacks in the mobile platforms. It is very difficult to identify the exact format of application in Mobile screen. Hence, Vulnerability of phishing in Smartphone is more. In the phishing mobile Applications the users are tricked to provide sensitive personal financial Information. First time users are more prone to Phishing attacks.

Prevention against Phishing attacks

- PPI Service providers need to provide their full contact details in the Android app store.
- The customers should be given sufficient warnings against spear phishing.
- The users are supposed not to share any of the personal financial information through e-mail.
- SSL (secure socket layer) and TLS (Transport layer Security) should be adequately implemented in mobile banking Apps.

ARP spoofing attack in Wi-Fi routers

The association of IP addresses into physical addresses is done through Address Resolution Protocol (ARP). It is used for the resolution of network layer address into data link layer address. When a reply is inconsistent with the currently cached ARP reply, the ARP replies are need to be blocked and alarm needs to be raised.

- The feature of port security can be enabled.
- Basically unsolicited ARP replies needs to be blocked and alarm needs to be raised when a reply is inconsistent with the currently cached ARP reply.
- VLAN can be used to limit the exposure.
- By using DHCP snooping and Dynamic ARP Inspection (DAI) features, ARP spoofing can be avoided.
- Consider using protocols such as EAP-TLS, IEEE802.14,AAA mechanism, to present such attacks.

Attack on SMS based OTP

There is a vulnerability of SMS based OTP. Sometimes it may also get hacked. Eavesdropping, intercepting and forwarding of SMS messages anywhere along the path between the sender and receiver.

Prevention against hacking of OTP

- Providing end-to end encryption for the SMS through OTP.
- Augmenting separate dedicated SMS OTP channel may also be explored.

Man in the middle attack (MIMA) through Home Node B

The Home Node B and femto cell configurations can be used to improve the coverage in a small area. It can also be used for providing in building solution (IBS). By exploiting the weak security mechanism involved in the Home Node B and femto cell configurations there is a possibility of launching man in the middle attack across smart phone data connections.

Prevention of MIMA through Home Node B and femtocell

- Using suitable end to end encryption mechanism.

Vulnerabilities in Biometric based authentications

Biometric is unique to an individual and it is very sensitive information. Hence, it needs to be protected with the highest standard of security mechanism. Biometric based authentications provide different kind of vulnerabilities. It is possible to lift the latent finger print with advanced technology and specialised chemicals. Though it is difficult, it is possible to intercept the biometric details like finger print.

Prevention of Biometric based vulnerabilities

- It is essential that biometric data needs to be encrypted immediately at the time of capture on the capturing device.
- The biometric data collected must not be stored in the device or log files.
- All the SSL communications should automatically validate the SSL certificate and ensure that it is validated against the online revocation list.
- In order to strengthen the security, multiple authentication factors such as PIN, OTP, demographic data or combinations thereof can be used along with biometric data.

SS7 based attacks

The weakness in the telecommunication protocol SS7 can also be exploited to launch attacks. The whole of the telecom networks authentication and security is based on the security of such protocols. The security breach in the network allows hackers to track the call and SMS details. Even denial of services can also be launched with the attacks.

Safe guarding against SS7 based attacks

- Never share sensitive personal financial information like Debit card nos and credit card nos, M-pin, OTP through SMS.
- The PPI/banking service providers should always provide their own robust end to end security mechanism for their digital payments.

Smishing

It is Short Message Service (SMS) based Phishing. The scammers will try to send text SMS as if it has originated from the bank/ PPI service providers by providing various credit card/ debit card details and user ids. The SMS may be asking for sending some sensitive details.

For prevention of Smishing based attacks

- It case of any such SMS seeking sensitive financial information, the customer should not respond for the SMS and they should try to contact their service banks/PPI service providers and inform about the SMS.
- Never share sensitive personal financial information like Debit card nos and credit card nos, M-pin, OTP through SMS.

Zero-day Vulnerabilities

The Zero-day vulnerability is a security loop hole in the application which exists at the time of releasing the application which is unknown to the PPI service providers. This offers attackers scope for attacking and exposing the vulnerabilities. The hackers may use it for cyber heist. This may sometimes cause huge embarrassment to the service providers.

Prevention Practices

- Code obfuscation may be used by the service providers to hide intellectual property and to thwart reverse engineering.
- The application needs to undergo all kind of testings like vulnerability assessment, penetration testing and third party application security testing etc including detailed certifications etc.
- As far as possible all, security and encryption techniques needs to be embedded in applications

Botnet attacks: -

It is a network of computers infected by malwares such as Computer virus, worms etc. It can also be controlled remotely by hackers for financial gains and to launch attacks on websites and infrastructures. The botnet attacks may try to gain access of Debt card, credit card related information and PIN numbers, OTP etc.

Prevention against Botnet attacks

- The Internet Bandwidth with the PPI service providers can be effectively monitored in coordination with the Internet service providers (ISPs) so that based on the traffic pattern origination; malwares can be identified and eliminated.
- Round the clock real time based enhanced traffic monitoring.
- virtual Local Area Networks (VLANs) and access control lists between sub networks may be used to limit exposure.
- Botnets may try to establish communications with external networks (i.e) with one or more remote servers. Hence, the traffic needs to be identified and filtered suitably through egress filtering.
- Monitoring Responses for DNS queries such as very low TTL (Time to live) value etc.

Best practices to remain safe

1. Always it is best to follow standard security guidelines and best practices followed in the industry.
2. Following e-KYC norms and periodical verification of e-KYC norms.
3. Authentication is the first line of defence which can filter out any kind of vulnerabilities in the channels. Hence, suitable design of authentication flow according to the back end data design is required. Hence, following up of at least two factor authentications (2FA) at all levels may be followed. In addition to the 2FA, some innovative authentication procedures will be helpful to solve the vulnerabilities.
4. Most of the breaches in the financial sectors are happening due to identity theft. Hence, sufficient and regular awareness about dos and don¿ts needs to be provided to their customers with all modes of communications.
5. Cyber security is not only IT related matters. It is a business related matters. With the rampant exposure to vulnerabilities, huge attention on the continuous preparedness is mandatory.
6. Use always updated software, Mobile OS and browsers.
7. Installing effective antimalware software at the user devices.
8. Overall enhanced Mobile Device Management (MDM) and security functionality needs to be followed at the user level.
9. Though mobile carrier provides good encryption between BTS and mobile devices, the PPIs have to ensure the security of the whole network up to the payment gateway servers.
10. Always use comprehensive and reliable mobile security solutions.
11. Strengthen networking infrastructures as per standard security guidelines of organisation.
12. Public Wi-Fi networks should not be used for accessing email, online banking and Credit Card accounts or any other sensitive data for that matter.
13. PPIs must have risk assessment policies and procedures, information security & management policy.
14. Specific recommendations with respect to threats and vulnerabilities needs to be issues regularly.
15. Sensitive personal information should not be stored during processing.
16. In payment mobile applications, QR code needs to be created within the Mobile application to ensure secure financial transactions.
17. Applications that use Aadhaar Authentications on various end user devices must comply with the specifications issued by UIDAI to protect all the biometric and demographic information provided by residents.

References

http://searchsecurity.techtarget.com/answer/How-can-vishing-attacks-be-prevented
https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls
https://www.sans.org/reading-room/whitepapers/critical/fall-ss7--critical-security-controls-help-36225
https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/fake-banking-app-android-malware/
http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html

https://uidai.gov.in/images/mou/data_protection_and_security_guidelines_for_registrar.pdf

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India