certin Handling Computer Security Incidents
Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2016-0063

Security of Micro ATMs

Original Issue Date: November 28, 2016

Systems Affected

- Micro ATMs

Description

Micro ATMs are Point of Sale (PoS) Devices that work with minimal power, connect to central banking servers through GPRS, thereby reducing the operational costs considerably. Micro ATM solution enables the unbanked rural people to easily access micro banking services in a very effective manner.

The basic interoperable transaction types that the microATM will support are:

1. Deposit
2. Withdrawal
3. Funds transfer
4. Balance enquiry and mini-statement.

The microATM will support the following means of authentication for interoperable transactions:

1. Aadhaar + Biometric
2. Aadhaar + OTP
3. Magnetic stripe card + Biometric
4. Magnetic stripe card + OTP
5. Magnetic stripe card + Bank PIN

Threats to Micro ATMs

Data Vulnerabilities

With respect to POS data vulnerabilities, there are three specific areas that should be given attention including data in memory; data in transit; data at rest. Data in memory in this context is when the card track data is brought into the system at the POS system via a POI (Point of Interface or some other input device). Data in memory is nearly impossible to defend if an attacker has access to the POS system. Traditionally, data input into the POS system was in memory in clear text, which is what allowed, attackers¿ memory scrapers to be very successful. The way to minimize this risk is by encrypting the card data as soon as possible and keeping it encrypted to the maximum extend throughout its life within the system. Point to Point Encryption (P2PE) could be used to address the issue of encrypting data in memory.

Skimming

Skimming is the theft of credit card / Debit card information. Thief can obtain victim's credit card number using a small electronic device near the card acceptance slot and store hundreds of victim's credit card numbers.

Social Engineering

Social engineering involves gaining trust - hence the fraudster poses as a member of staff. The fraudster would then ask the customer to check the card for damages. The fraudster would have gained confidence from his prey using various tactics such as offering assistance to the customer who perhaps would have tried to use the ATM without success or perhaps the customer who is not familiar with use of micro ATM machine and requires assistance.

Best Practices for Users

- Before using micro ATM, please ensure that there are no strange objects in the insertion panel of the ATM(to avoid skimming)
- Cover the PIN pad while entering PIN. Destroy the transaction receipts securely after reviewing.
- Change ATM PIN on a regular basis.
- Keep a close eye on bank statements, and dispute any unauthorized charges or withdrawals immediately.
- Shred anything that contains credit card number written on it. (bills etc)
- Notify credit/debit card issuers in advance for change of address
- Do not accept the card received directly from bank in case if it is damaged or seal is open.
- Do not write PIN number on credit/debit card.
- Do not disclose Credit Card Number/ATM PIN to anyone.
- Do not hand over the card to anyone, even if he/she claims to represent the Bank.
- Do not get carried away by strangers who try to help you use the microATM machine.

- Do not transfer or share account details with unknown/non validated source.
- In case of any suspected transactions or loss of cards, contact the service provider / bank immediately.

Best Practices for Service Providers

- The microATM must not transmit any confidential data unencrypted on the network.
- The microATM must automatically log out the operator and lock itself after a period of inactivity.
- Keep all the microATM software, application, antivirus regularly updated.
- Educate the customer about basic functionalities and security best practices.

References

CERT-In
Security of POS Systems (CIAD-2016-62)
http://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2016-0062

IBA
http://www.iba.org.in/upload/MicroATM_Standards_v1.5.1_Clean.pdf

NPCI
http://www.npci.org.in/documents/Procedural_Guidelines1.pdf

UIDAI
https://uidai.gov.in/images/commdoc/microatm_standards_v1.4.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