CS
Assignment 2

Submitted By:-
Aman Chauhan
D3 CSE A1
1805158

Q1. Explain Micro ATM Security.

Ans. 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 micro ATM will support are:

- Deposit
- Withdrawal
- Funds transfer
- Balance enquiry and mini-statement.

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

- Aadhaar + Biometric
- Aadhaar + OTP
- Magnetic stripe card + Biometric

- Magnetic stripe card + OTP
- Magnetic stripe card + Bank PIN

Q2. Explain Social Engineering And Its Types?

Ans. Social engineering, once mastered, can be used to gain access on any system despite the platform or the quality of the hardware and software present. It‘s the hardest form of attack to defend against because hardware and software alone won‘t stop it. It can be defined as an outsider tricking legitimate personnel into aiding illicit acts such as supplying proprietary information or allowing inappropriate access. It preys on the weakest link in a security system- the human being.

TYPES:

<u>Physical Social Engineering:</u>

In a physical social engineering attack, the social engineer attempts to gain access to a physical location. The attacker may do this via various methods, including :

- Piggybacking: Used to enter restricted area by convincing an authorised personal.
- Eavesdropping: Attacker can gain information by hearing a discussion between two people,

or by reading emails and listening to telephonic conversation.

- Impersonation: The attacker acts like someone else to trap the victim
- Dumpster Driving: Valuable information can often be found on trash, printers and pieces of paper.
- Reverse Social Engineering: It is a more advanced method. In this the attacker creates a scenario where the victim ends up asking for information to the attacker and in this process ends up providing the required information to the attacker. Typically the

attacker appears to be in a position of authority to ensure the victim has to reach out to him for resolution of a problem which the attack has set up for him. Reverse social engineering requires good pre- attack research and planning, however if executed well it is more successful in attaining gaining quality information.

Remote Social Engineering:

Remote social engineering involves pointed and real-time communication with the target over the phone or via email or via instant messaging. This uses items planted to lure employees to run payloads.

- Computer-based Social Engineering Computer based social engineering is implemented by using software or programming applications like E-Mails, IM, websites, pop-ups.
- Social Engineering by Email Social engineering emails take many forms. The

social engineer tries to build rapport as a precursor to the actual breach, or she tries to elicit information or spread malware by tricking theemail recipient into opening a malicious attachment or visiting a malicious website. Two of the most common forms of social engineering over email are phishing and 419 scams.

Q3. Why UPI Security Is Essential.

ANS.

- With UPI, a user's bank account can be used as a wallet with a simplified two-factor authentication which eliminates the need to store funds in any other wallet.
- Use of Virtual ID makes it more secure since there is no need to share credentials.
- UPI transaction can be made via IMPS in real time, which makes it available 24*7.

- Users can link multiple bank accounts to a single Smartphone. Hence sending or receiving money across banks is easier.
- For merchants, it is Suitable for electronic Commerce and a mobile Commerce transaction as well as it resolves the Cash on Delivery collection problem.
- Banks can create their own application interfaces as UPI provides flexibility and an open architecture.

Q4. List Out The Functions Of Ccleaner.

ANS.

- Remote optimization of Endpoints
- Auditing of Endpoint health
- Remote problem solving
- Scheduled cleaning and defragmentation
- Granular control of cleaning rules
- Simple one-click deployment onto Endpoints

- Highly-secure Endpoint agent and encrypted communications
- LDAP/Active Directory support
- Built-in reporting and auditing tools with data export

Q5. What Is Mobile Banking Security.

ANS. The increasing usage of Smartphones has enabled individuals to use various applications including mobile banking applications. More and more individuals have started using mobile applications for banking as compared to the traditional desktop/Web-based banking applications.

Best Practices For Users To Remain Safe:

- Enable Passwords On Devices: Strong passwords should be enabled on the user’s phones, tablets, and other mobile devices before mobile banking apps can be used. Additional layers of security inherently provided by these devices should be used.

- Bank account number or IPIN should not be stored on the user’s mobile phone.
- The user should report the loss of mobile phone to the bank for them to disable the user's IPIN and his access to the bank's account through Mobile Banking app.
- When downloading the Bank’s Mobile app in the mobile device, the user should go to a trusted source such as the App Store on the iPhone® and iPod touch® or Android Market. User can alternately check the Bank’s website for the details of the ways to receive App download URL, whether in the response to his SMS or email to the bank and then install the application. The app from any other third party source should not be downloaded.