Presenting Abuse/Misuse Cases for an Automated Teller Machine (ATM)

A Report By

Mark Kardash

SDEV360: Secure Software Engineering

Professor David Gabello

8 November 2023

University of Maryland Global Campus

**Discussion of Misuse/Abuse Cases for ATM**

An Automated Teller Machine (ATM) is a device intended to help the user with financial transactions. However, users may sometimes, either intentionally or unintentionally, handle the device in ways different from those it was designed for. This could either be done due to a customer lacking the knowledge of how to interact with the ATM, or due to a hacker wanting to obtain sensitive information. Since ATM machines work with finances, they store a lot of sensitive data that is very lucrative to attackers. This could include a customer’s name, credit card number, banking information, various addresses, and other details. Instances of an application’s incorrect use are known as abuse or misuse cases. They can occur in any stage of an application’s working process, and manifest in many different ways. Some of them may be based on regular use cases, but with steps altered to include malicious actions. This paper will examine the abuse and misuse cases for an ATM, as it processes a customer’s credit card.

The first stage of an ATM’s use is the System Startup, during which the customer activates the machine, and makes necessary selections to begin a session. For this case, as well as for those following it, three hypothetical entities will be involved: The customer, the operator, and the attacker. The use case for the startup stage unfolds as such:

1. Customer pushes button to turn on the ATM.
2. Operator prompts customer to select their desired bank.
3. Customer selects bank.
4. Customer inserts debit or credit card into ATM.

Although this initial stage may seem very short and relatively safe, there are several opportunities for hackers to strike here. First, the above steps do not give an opportunity to verify the identity of the ATM operator. While the customer may trust without much doubt that the bank will keep their data safe, it is not uncommon for hackers to have “their own person” within the organization they are targeting. They could either be a bank employee, or pass as an ATM maintenance worker, and tamper with the machine. Without proper authentication, anyone with knowledge of the ATM functions can gain access to customer data. Using an external device or cable (ex. One installed during the supposed “maintenance”), the attacker can send the data entered by the customer to a server separate from that of the bank (Snow, n.d.). Therefore, a misuse case at the Startup stage may look like this:

1. Operator (who is, in fact, a hacker) uses a key to open the chassis of the ATM. This exposes the cable responsible for the bank network). (Snow, 2016).
2. Operator disconnects ATM from the bank network (Snow, 2016).
3. Operator connects ATM to their own separate network using a special device (Snow, n.d.).
4. Customer activates ATM.
5. Customer selects desired bank.
6. Customer inserts debit or credit card.
7. Operator uses a skimmer, a device specially designed to read data from the card (Iven, 2022).
8. Since the ATM is now connected to the attacker’s own network, all the data, such as customer’s name, PIN, card number, etc., gets stored there. The attacker can now access it, and easily retrieve any money from the card.

The above scenario will, obviously, have disastrous consequences both for the customer and the bank. The former will fall victim to data theft, perhaps even identity theft, while the latter will be held responsible for not doing enough to prevent it. To avoid this, there are several ways in which the situation described can be prevented. Firstly, it is advisable for all banks to require operator identity verification on their ATMs. The authentication can be requested in the form of a username and password that only a single employee knows. The website IT Security Guru recommends that “passwords should be changed at least every 90 days and should be at least 14 characters long, incorporating at least one number, both upper and lower case characters, and non-alphanumeric characters.” (Rule 2, para.2, 2018). While this method may not prevent an employee insider from accessing the system, it will eliminate the ways hackers can infiltrate it from outside.

Another popular way of protecting ATMs from attacks at the startup stage is encrypting customer data. Even if the cybercriminal uses a skimmer or other special device, they will be unsuccessful in reading card information during transactions. This method is often made a requirement by companies, due to its high efficiency in protecting sensitive cardholder information (IT Security Guru, 2018).

The System Startup stage is followed by the more complicated Session stage, during which the customer performs their desired operations on the ATM, including the transaction. There could be three use cases for this stage, and each of them continues from where the Startup stage left off:

Use Case 1:

1. Customer inserts debit or credit card into ATM.
2. ATM does not recognize the card.
3. Card is ejected. Operation is cancelled.

Use Case 2:

1. Customer inserts debit or credit card into ATM.
2. ATM recognizes the card.
3. Operator prompts customer for a PIN.
4. Customer enters invalid PIN.
5. ATM rejects invalid PIN. Operation cancelled.

Use Case 3:

1. Customer inserts debit or credit card into ATM.
2. ATM recognizes the card.
3. Operator prompts customer for a PIN.
4. Customer enters PIN.
5. PIN recognized. Customer prompted to execute operation of choice (Withdrawal, Deposit, Transfer, Inquiry).
6. Customer can either select and complete an action or cancel their progress at any time.

At the Session stage, the threat level increases for customer data. The attackers can intercept the PIN entered by the customer using password-guessing attacks, or the very popular brute-force attack. Successfully guessing the PIN means gaining access to the customer’s card, and all the valuable information on it. As such, a Session misuse/abuse case could look like this:

1. Customer inserts debit or credit card into ATM.
2. ATM recognizes the card.
3. Operator prompts customer for a PIN.
4. Customer enters valid PIN.
5. Attacker launches a brute-force attack.
6. Brute-force attack is complete. PIN has been guessed.
7. Attacker uses PIN to access customer’s financial information.

As with the Startup attack, the interception of a PIN by hackers, and the subsequent leak of financial data, can have a disastrous impact on both the bank and its customers, entailing everything from legal issues to bankruptcy. In terms of mitigation, previously mentioned methods like encryption and authentication will certainly help keep the PIN safe. In this case, it is recommended that “all user accounts and passwords for every ATM machine must be different so the successful hacking of one does not lead to the hacking of another” (IT Security Guru, Rule 2, para.2, 2018). Also, the ATM must display an error message after each unsuccessful login and lock the user out after a certain number of attempts is reached.

In addition to the already discussed protection methods, a firewall can also be recommended for installation. A firewall will control the connections that are made to the ATM, and only permit those that are needed. For effective protection, the bank must ensure that the firewall is configured correctly (IT Security Guru, 2018). An effective tool against brute-force attacks is the Config Server Firewall (CSF). The CSF allows the user or organization (In this case, the bank) to control traffic within the system, see the activities of users, and monitor who enters it (AccuWeb Hosting, 2023). Therefore, a firewall is very beneficial to an ATM, and to the bank responsible for it.

The next phase of using an ATM is not so much a separate phase, as it is a step in the session. It is called the Transaction stage, and it is when the customer performs their desired financial actions. Below is a potential use case for this stage:

1. Customer is presented with four options of what to do with their finances (Withdrawal, Deposit, Transfer, Inquiry). Here, there are four potential scenarios:

Scenario 1:

* 1. Customer selects withdrawal.
  2. Operator prompts for withdrawal amount.
  3. Customer enters and confirms withdrawal amount.
  4. Amount is given to customer in cash.
  5. Card is returned (ejected) to customer. Operation is completed.

Scenario 2:

* 1. Customer selects deposit.
  2. Operator prompts for deposit amount.
  3. Customer enters and confirms deposit amount.
  4. Deposit is successfully made. Confirmation message appears.

Scenario 3:

1. Customer selects transfer.
2. Operator prompts to select account to transfer to.
3. Customer selects account.
4. Operator prompts for amount of funds to be transferred.
5. Customer enters fund amount.
6. Customer confirms transfer.
7. Confirmation message appears. Transfer completed successfully.

Scenario 4:

1. Customer selects inquiry.
2. Operator displays balance of customer’s account. Operation completed successfully.

Of course, there are some common dangers that could strike in any of those four cases. The biggest issue is that, in all four of them, critical information about the user’s (customer’s) account is viewed. This is perhaps the best time for an attacker to strike, since, while the data is vulnerable at that moment, a multitude of different attacks can be performed, from data theft via skimmer to retrieval of funds on the card. A potential misuse/abuse case for the Transaction stage would be:

1. Attacker disconnects ATM from bank server.
2. Attacker connects ATM to their own separate server.
3. Customer is prompted with four options on how to proceed (Withdrawal, Deposit, Transfer, Inquiry).
4. Customer selects Deposit.
5. Rather than being deposited into the bank, the costs are deposited into the attacker’s own server.

As a consequence of the above scenario, the customer loses their money, while the attacker has completed a successful illicit operation. Mitigation of this problem would involve displaying no more information than necessary to complete the action chosen by the user. Additionally, to ensure that the customers has considered each of their actions well, the ATM should request them to confirm each action they take. This will allow to cancel the process at any time, keeping the data safe.

**Research on Personally Identifiable Information**

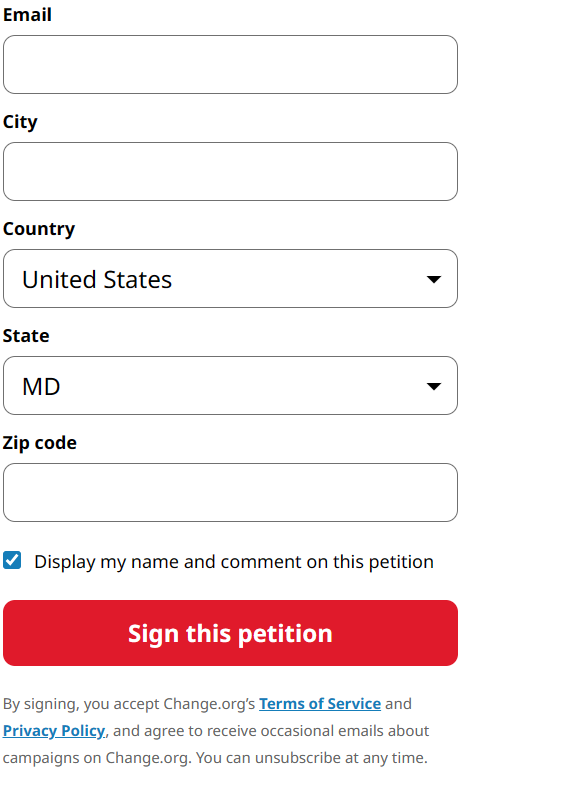
In my life, and especially since I came to the United States, I have had to fill out a multitude of forms. They requested an enormous amount of information, some of which seemed excessive, and even unreasonable to me. However, I must clarify that I am unsure whether they were in fact unreasonable, or if it seemed so to me due to not being accustomed to certain American regulations. Still, this always made me a bit concerned about the safety of my Personally Identifiable Information (PII). According to IBM (n.d.), personally identifiable information “is any information connected to a specific individual that can be used to uncover that individual's identity, such as their social security number, full name, or email address.” (para.1). As I learned more about this type of data over the years, I have learned to avoid suspicious sites by knowing what information is usually requested (Ex. A legitimate language learning website will never ask for our social security number). However, in some cases, even legitimate applications ask for information that serve no purpose in the context of the form. Some examples of this would be:

Asking for a primary phone number on an online store’s checkout page (Carlton, 2015).

Asking for a customer’s gender on an e-commerce order form.

Asking for secondary email addresses or phone numbers when not needed for a valid reason (ex. Account backup).

An example I have personally encountered is when a petition website, Change.org, asked me for my physical address. While I understood their requests for name and email, I frankly do not see a reason why my physical address would be needed. In fact, some of the fields are already completed by the website when I get there. I believe that it tries to guess my location, which it fails in, but falls very close.



**Figure 1:** Physical Address of Residence being asked on Change.org (Source: https://www.change.org/p/build-a-replica-of-the-rms-olympic)

Above, the request for a physical address by the website Change.org is shown. I have removed the pre-filled information from the fields, but the fields “City” and “Zip Code” already contain data when the user accesses the site. There are several problems with websites asking for unnecessary data from their customers. The first is that, as already mentioned, the customer may not feel comfortable with sharing it. The request for data they are not comfortable with sharing may cause some people to abandon using the site. This, in turn, will cause the company owning it to lose customers. This can be worsened by the fact that some clients may feel they are treated as marketing targets, and not valued enough as individuals (Kedinger, 2016). Once this belief spreads, customer trust in the company will fall significantly.

Collecting unnecessary data can not only be harmful, but dangerous as well. If the company or organization in question falls victim to a cyberattack, all this PII can end up in the hands of attackers. There is a multitude of ways it could then be used, from financial frauds to identity theft, especially if it involves such sensitive data as a Social Security Number.

The first step in preventing issues like this is for companies to reassess what they need from each customer. This may mean completely reevaluating, and redesigning, their Information and Privacy policies. If a secondary address or phone number plays no role in the desired outcome of filing a form, it should not, for any reason, be included there. Kedinger (2016) also recommends using a practice known as progressive profiling, which “which will ask additional questions after a user has visited a form multiple times” (para.4).

If I were a company employee and felt that the company was asking unnecessary information from its customers, I would advance the issue to the higher ranks, and respectfully address it in a conversation with my supervisor. In my conversation, I would address exactly what information I believe to be unnecessary, and explain the ways requesting it can harm the organization in the future.

References

*Build a Replica of the RMS Olympic*. (n.d.). Change.org. <https://www.change.org/p/build-a-replica-of-the-rms-olympic>

Charlton, G. (2015, December 18). *Web form design: Eight common mistakes to avoid*. ClickZ. <https://www.clickz.com/web-form-design-eight-common-mistakes-to-avoid/23053/>

*How to protect ATMs against logical attacks*. (2018, March 29). IT Security Guru. <https://www.itsecurityguru.org/2018/03/29/protect-atms-logical-attacks/>

Iven, A. (2022, March 8). *Protect your ATM machine with these 5 ATM security tips*. ATM Depot. <https://atmdepot.com/atm-security-tips/>

Keninger, D. (2022, December 7). *7 mistakes to avoid when designing website forms*. Practical Ecommerce. <https://www.practicalecommerce.com/7-Mistakes-to-Avoid-When-Designing-Website-Forms>

Snow, J. (2016, September 29). *4 ways to hack an ATM — video*. Kaspersky Cyber Security Solutions for Home and Business | Kaspersky. Retrieved November 8, 2023, from <https://www.kaspersky.com/blog/4-ways-to-hack-atm/13126/>

*Top 5 Tools for Preventing Brute Force Attacks*. (2023). AccuWeb Hosting. Retrieved November 8, 2023, from <https://www.accuwebhosting.com/blog/prevent-brute-force-attacks/>

*What is personally identifiable information (PII)?* (n.d.). IBM - United States. <https://www.ibm.com/topics/pii>