Project: Requirements Misuse and Abuse Cases

Benjamin M. Brandhorst

University of Maryland Global Campus

SDEV 360 6380 Secure Software Engineering

Professor Kevin Woodson

February 2nd, 2020

Project: Requirements Misuse and Abuse Cases

Automatic Teller Machine (ATM) abuse/misuse case:

System Startup Misuse Case: While the system is in the startup process, there are no methods in place to authenticate the operator. Because the ATM makes a connection to the bank network, it may be possible for a malicious user to use the operator panel to access personally identifiable information (PII) and other banking information.

Possible Mitigations: One way to mitigate against this vulnerability would be the use of a physical key and username/password combination, designed in a way that will lock out the operator after a reasonable number of incorrect entries.

System Shutdown Misuse Case: After the system is shut down, it may be possible for the operator to falsify the amount of cash within the ATM. There are no physical barriers that would prevent the operator from taking money out of deposits or the cash dispenser.

Possible Mitigations: One possible mitigation strategy could be a system in which detailed transaction records are reported electronically and a physical printout is created which would accompany the deposit slips to be verified by a third party.

Session Misuse Case: When a customer is asked to enter his or her personal identification number (PIN), the ATM software is vulnerable to an attack using the brute force or dictionary attack methods. In both of these cases, the pin number is entered multiple times until the malicious actor successfully uncovers the correction combination of numbers associated with the card inserted.

Possible Mitigations: The ATM software, as currently designed, attempts to mitigate against this type of attack by locking customers out of the ATM kiosk and retaining possession of their bank card if the threshold of three incorrect PIN entries has been met.

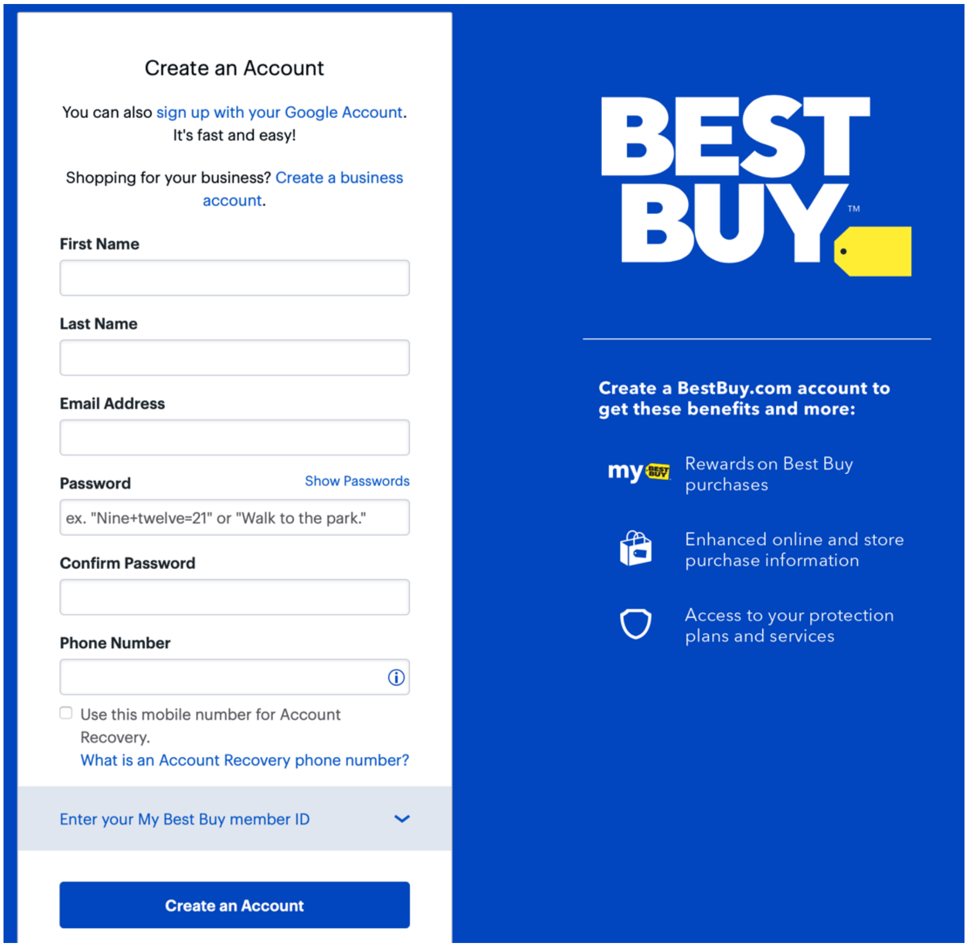
Transaction Misuse Case: When a customer chooses a transaction type the network the ATM operates on is vulnerable to an attack. One such attack would be a processing center spoof. Absent a secure network, the data between the ATM and the processing center on the bank network is vulnerable to manipulation. A malicious user can connect an emulated processing center to the ATM that approves all transaction requests. This will allow the user to empty the contents of the ATM without the machine communicating with the bank to deduct money from any accounts.

Possible Mitigations: This vulnerability can be mitigated with a combination of strategies. First, all data to and from the ATM should be encrypted using the strongest end to end encryption methods reasonably available. Secondly, message authentication codes should be used in both transaction requests and responses. Finally, virtual private network (VPN) hardware and software should be secured. If VPN hardware is used, it should be placed in such a way that an attacker is unable to install their own equipment between the ATM and VPN.

PII Research:

PII is defined as “information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual” (The United States Government, 2019, § 200.79). The collection and storage of PII presents a risk to both the owner of said PII and the business or agency that maintains those records. I have gathered some examples of website forms that gather more information than is needed and will go through them below.

Example #1



Create an Account

You can also sign up with your Google Account. It's fast and easy!

Shopping for your business? Create a business account.

First Name

Last Name

Email Address

Password Show Passwords

ex. "Nine+twelve=21" or "Walk to the park."

Confirm Password

Phone Number

□ Use this mobile number for Account Recovery.
What is an Account Recovery phone number?

Enter your My Best Buy member ID

Create an Account

BEST BUY™

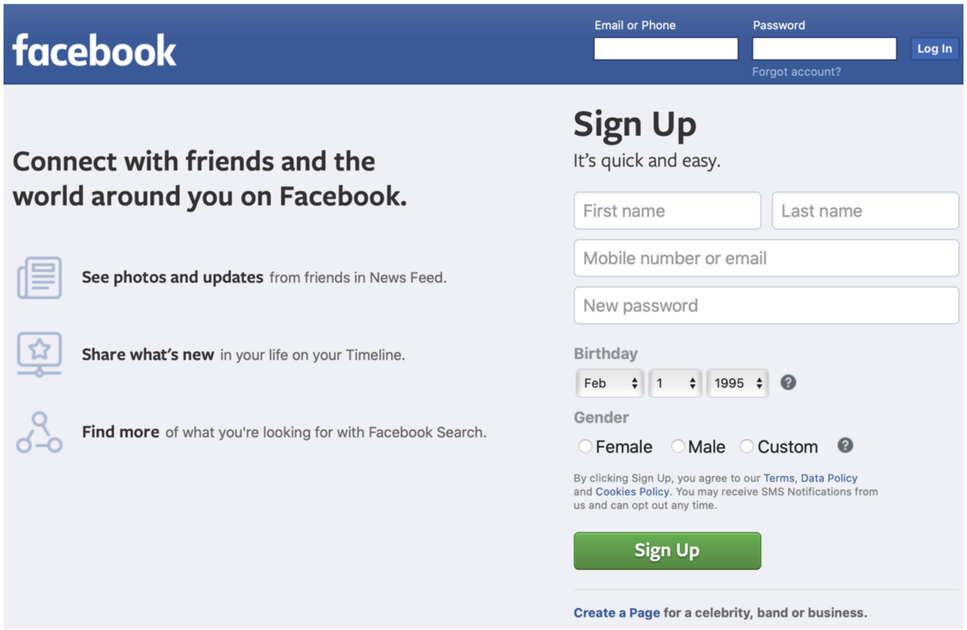
Create a BestBuy.com account to get these benefits and more:

- Rewards on Best Buy purchases
- Enhanced online and store purchase information
- Access to your protection plans and services

Figure 1 – My Best Buy account creation (source: www.bestbuy.com)

When using the Best Buy “My Best Buy” account signup, users are prompted to enter their full names, email address, and phone number. A phone number should not be required for this account. While Best Buy may gather this information to create a more detailed customer profile by linking this with other information gathered, it is not specifically required to process the “My Best Buy” account creation request.

Example #2



Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

Share what’s new in your life on your Timeline.

Find more of what you're looking for with Facebook Search.

It’s quick and easy.

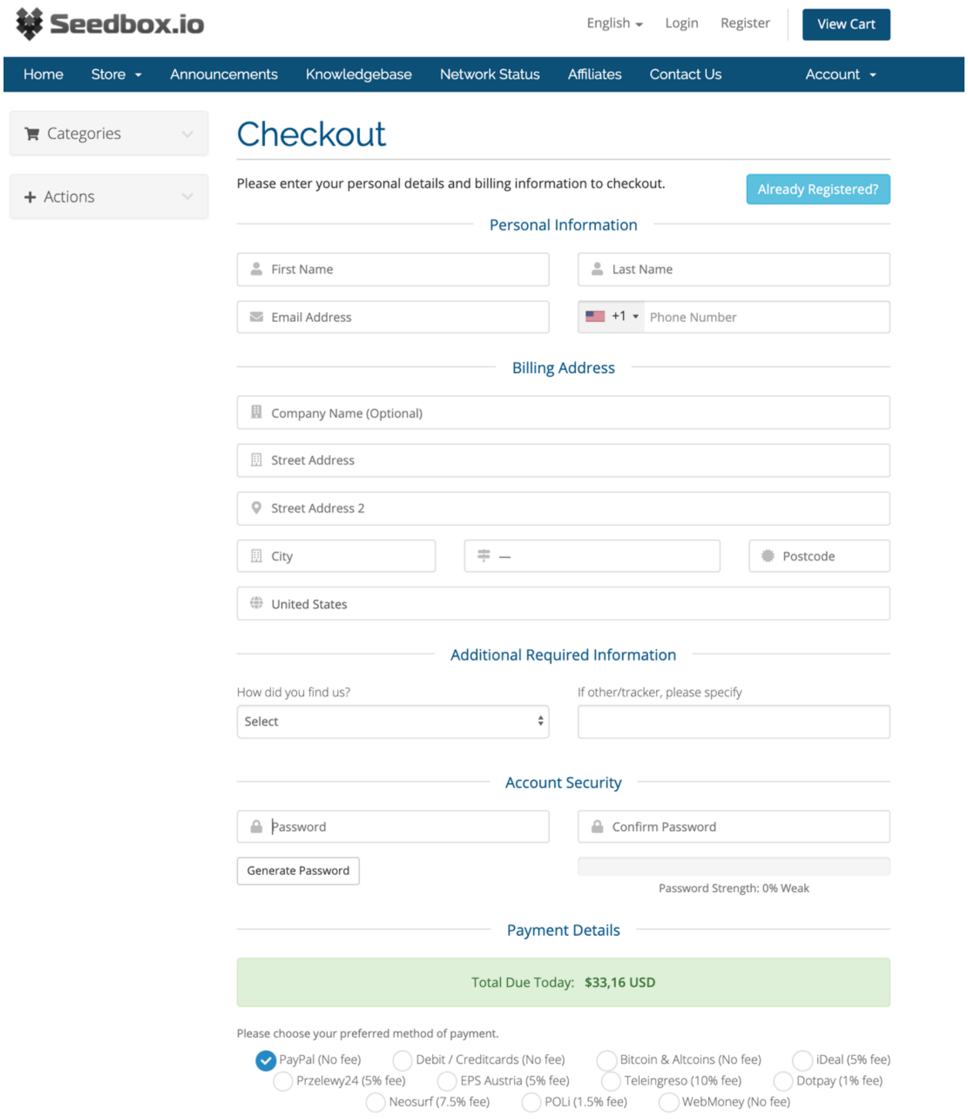
By clicking Sign Up, you agree to our Terms, Data Policy and Cookies Policy. You may receive SMS Notifications from us and can opt out any time.

Create a Page for a celebrity, band or business.

Figure 2 – Facebook account creation (source: www.facebook.com)

When signing up for a Facebook account, users are prompted to enter their full name, cellular phone number or email, birthday, and gender. This information and more is stored and used to create a profile that Facebook uses for advertisement targeting.

Example #3



Checkout

Please enter your personal details and billing information to checkout.

Personal Information

First Name | Last Name

Email Address | +1 Phone Number

Billing Address

Company Name (Optional)

Street Address

Street Address 2

City | — | Postcode

United States

Additional Required Information

How did you find us? Select

If other/tracker, please specify

Account Security

Password | Confirm Password

Password Strength: 0% Weak

Payment Details

Total Due Today: **$33,16 USD**

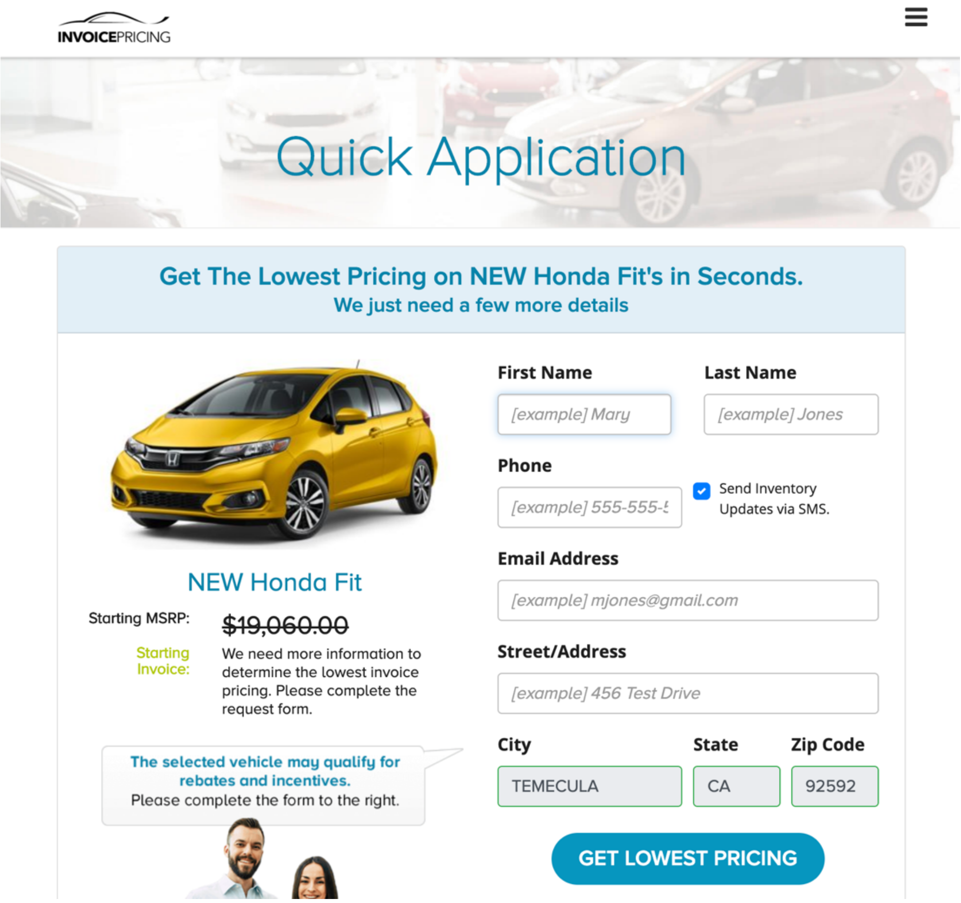
Please choose your preferred method of payment.

● PayPal (No fee) ○ Debit / Creditcards (No fee) ○ Bitcoin & Altcoins (No fee) ○ iDeal (5% fee)
○ Przelewy24 (5% fee) ○ EPS Austria (5% fee) ○ Teleingreso (10% fee) ○ Dotpay (1% fee)
○ Neosurf (7.5% fee) ○ POLi (1.5% fee) ○ WebMoney (No fee)

Figure 3 – Seedbox.io checkout page (source: https://seedbox.io)

Seedbox.io is a website that rents specialized servers configured for bit torrent use. While there are completely legitimate and legal reasons for someone to use a seedbox, they can also be used for illegal purposes such as pirating electronic media. Many other seedbox hosts collect only the bare minimum information required to process transactions for their customers. However, Seedbox.io requires full name, mailing address, and phone number for all customers even if they are paying with PayPal or crypto currency.

Example #4



INVOICEPRICING

Quick Application

Get The Lowest Pricing on NEW Honda Fit's in Seconds.
We just need a few more details

NEW Honda Fit

Starting MSRP: ~~$19,060.00~~

Starting Invoice: We need more information to determine the lowest invoice pricing. Please complete the request form.

The selected vehicle may qualify for rebates and incentives.
Please complete the form to the right.

First Name	Last Name
[example] Mary	[example] Jones
Phone	
[example] 555-555-5	☑ Send Inventory Updates via SMS.
Email Address	
[example] mjones@gmail.com	
Street/Address	
[example] 456 Test Drive	

City	State	Zip Code
TEMECULA	CA	92592

Figure 4 – Invoice Pricing inquiry page (source: www.invoice-pricing.com)

Invoice Pricing is a website which promises to help users find the best new vehicle deals by showing the invoice price on new model cars. However, when a user tries to view the invoice price for a vehicle, they are prompted to enter their full names, phone number, and mailing address to continue. None of this information is required to process the user's request.

The common theme with all of these websites is that they collect date of birth, phone number, and home address when this information is not explicitly required. This puts users at an increased risk because of the possibility of leaked information from a data breach. Additionally, this information is sometimes sold to advertisers who then send unwanted marketing text messages, email, and even regular old junk mail.

Users can try to mitigate the risks associated with providing this additional PII through a number of ways. One of these ways is using what is called a burner email address. This is typically a temporary email account set up specifically to get past a website requirement for providing an email contact. Another method is using an email address dedicated specifically for online accounts. Finally, users can attempt to enter a fake phone number and home address for most websites that do not ship physical items to them. However, this may be a violation of the site's terms of service and could result in unintended consequences.

The PII gathered from the above example websites is clearly valuable to the businesses that collect it. If I were to work for any of these companies, I would work towards redesigning the forms to limit the amount of information collected to only that necessary. Additionally, I would recommend we classify PII according to its sensitivity, delete old PII, and encrypt and pseudonymize all records. Once those things were in place, I would move on to developing employee education and policies regarding the protection of PII, creating a standard procedure for departing employees to ensure PII isn’t leaked if a disgruntled employee leaves, and developing a program in which employees can report suspicious behavior. These steps could help ensure our business remains in compliance with privacy protection laws in all fifty states and around the world.

References

ATM logic attacks: scenarios, 2018. (2018, November 14). https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/

Lakshmanan, R. (2019, September 10). Loyalty programs cost you your personal data. Are the rewards worth it? https://thenextweb.com/insights/2019/06/12/loyalty-programs-cost-you-your-personal-data-are-the-rewards-worth-it/

Lord, N. (2018, September 12). How to secure personally identifiable information against loss or compromise. https://digitalguardian.com/blog/how-secure-personally-identifiable-information-against-loss-or-compromise

TokenEx. (n.d.). PII tokenization and pseudonymization. https://www.tokenex.com/solutions/privacy-compliance

The United States Government. (2019). *Electronic Code of Federal Regulations*. Retrieved from Cornell Law School website: https://www.law.cornell.edu/cfr/text/2/200.79