Smart Mirrors: Privacy & Security Concerns

Navya Harika Karaka
Northeastern University
karaka.n@northeastern.edu

Abstract

Privacy and security are some of the main concerns in this growing data-driven technology. Over the past few years, due to several reasons such as poor design, in-sufficient privacy concerns and security compliance measures lead to compromised consumer's sensitive data on the Internet. Due to exponential growth in smart devices, the security challenges have also increased. In order to help mitigate some of these issues and to educate the people the importance of certain security features such as strong authentication, privacy rules, encryption etc., especially for people who might have not enough background in technology and smart devices, I propose a web-based/mobile-based application that allows its users to safely access all the smart-mirrors by providing certain security tips and also by monitoring these devices frequently. Although, this application will be mainly focused on smart mirrors for now, I plan to expand it to other smart devices in the near future. As part of the implementation process, I sent out few surveys and these surveys helped me understand the importance of this application. The main objective of this paper is to propose a solution and provide suggestions on how this application should be built and to suggest some key points to note while building the application.

Keywords—smart, devices, mirrors, privacy, security, application, consumers

I. INTRODUCTION

Over the past few months, smart mirrors have become very prominent. Although there are several kinds of smart mirrors that serve different purposes, in this paper, I will be focusing on one of the recent additions to smart mirrors in fitness industry i.e. Mirror. Mirror provides its users an unique interactive home fitness experience which became prevailing and trendy especially over the last few months during these unfortunate circumstances. This mirror provides several workout classes such as yoga, Pilates, strength training etc. [2] It looks very similar to a normal, modern-looking mirror that can be found in bedrooms, bathrooms etc. and it also contains several built-in cameras, voice-interactive tools etc. which allows its users to connect with a trainer or a fitness instructor to participate in group workout classes or training sessions. Similar to any other smart device, this mirror needs to be connected to the Internet either via Wi-Fi or Bluetooth in order to interact with it. Any device connected to the Internet is vulnerable and it could potentially be hacked. [1]

One of the reasons why I was intrigued by this mirror was mainly due to its data-driven technology. These mirrors collect and transmit significant amount of user's personally identifiable information (PII),including detailed whole body video capture, voice and audio capture, settings configurations, personal profiles, usage data, credit card information, banking information etc. Although there are similar concerns with other commonly used devices such as cell phones, cameras etc., I believe that there's not enough exposure about the security concerns about some of the latest smart devices such as smart mirrors etc. which increases the privacy and security concerns for the consumer.

The main objective is to address some of the security aspects of these smart mirrors and provide suggestions mainly to consumers who might not have enough background in technology in order to prevent potential security incidents.

II. PRIVACY AND SECURITY CONCERNS

A. Company-based security concerns

With the significant increase in smart devices such as smart refrigerator, smart mirrors etc. which mostly contain data-driven technology, the consumers and the companies were challenged to focus more on the security aspects by maintaining certain security compliance standards and by using proper privacy protocols, privacy settings, monitoring tools etc.

In order to ensure safety of consumer's data, following are *few* things companies can do: [4]

- Strong authentication
- Strong privacy rules
- Third-party monitoring and validation
- End-to-end encryption from the user device down to the database, application, and systems
- Roles-based access to data and systems
- Data classifications etc.

According to a recent article in Forbes, almost 2 billion consumer data records could potentially be exposed in case of a smart device breach. A smart device data breach could be due to several factors such as software vulnerabilities, network vulnerabilities, human-based security concerns etc. Since, these mirrors are heavily dependent on Wi-Fi and Bluetooth, there's a higher security concern since no smart device is really safe on the Internet.

B. User-based security concerns

Along with internet and software vulnerabilities, one of the main factors that increases the security concerns is the human-based errors. Based on several recent surveys, most people do not change their default passwords on the smart devices or they use most common passwords. Either default passwords or most common passwords could be found easily via powerful tools or via brute-force attacks. It's also important to note that most people do not update their smart devices by downloading the latest software updates that could potentially fix any existing or new software vulnerabilities. If a cyber-criminal somehow manages to get access to any of the built-in cameras in these smart devices, he/she can tilt the camera to monitor other activity in the house or if there other devices that are on the same network, then the hacker could potentially get access to the other devices as well. These are some of the reasons why security is a key concern in these smart devices.

In order to ensure privacy and safety of sensitive data, following are *few* things consumers can do: [5]

- Use strong passwords
- Disconnect/Turn off devices that are not in use
- Monitor any unauthorized activity
- Consider network segmentation
- Update software if required etc.

III. POTENTIAL CYBER ATTACKS ON SMART DEVICES SUCH AS MIRRORS

Cyber-criminals are always looking to explore and find new ways to hack devices and in recent years, smart devices became an easy target for cyber-criminals and hackers to exploit. With the amount and type of data that these smart devices store, there has been a significant increase in data breach risk and privacy and security threats.

Following are some of the threats that are common among smart devices: [5]

a) Unauthorized recordings: If an hacker somehow gets access to a smart device, he/she can potentially record all the conversations or video recordings without any authorization from the user and these recordings could be exposed.

b) Password exploitation: Most people tend to use default passwords or common passwords which could lead to potential brute-force attacks.

c) Location tracing: Location tracking is very common in most of these smart devices and companies take advantage of it to provide better user experience but if it falls into wrong hands, it could be harmful to the users.

d) Unauthorized data manipulation: If an hacker gets access to a smart device, he/she can manipulate data and expose it and demand ransom. There were several reports in past few years that lead to ransomware attacks.

e) Home intrusions: If an hacker or a potentially harmful gets access to smart device or location on your smart device, it could potentially lead to home intrusions and other harmful situations.

IV. ADDRESSING SECURITY CONCERNS

In order to mitigate some of these security concerns and to ensure and protect consumer's privacy to a certain extent, I plan to implement an application that can be used either on the web or on a cell-phone.

Following are some of the main objectives of this application:

- To help users register their smart devices such as fitness smart mirrors or skin-based smart mirrors and to manage these registered devices easily all in one place.
- It will monitor these registered smart devices and alert the users in case of any unusual activity to take necessary actions.
- It will also allow the user to shut down their registered devices directly from the application or set an auto-shutdown within certain time limit.
- Provide alerts every once in a while to educate users about the importance of use of strong password and multi-factor authentication.
- It will also alert users when there's any new software updates in order to fix any existing or new vulnerabilities.

V. IMPLEMENTATION PROCESS OF THE APPLICATION

Before I started the implementation process of the application, I sent out a few surveys to justify the security concerns of the smart mirrors and to determine if consumers would be interested in this application. The responses from the survey helped me understand the importance of these applications that allow consumers to easily access the smart devices which will allow the users to shut them down or update the software or change authentication.

During the planning process of this application and while researching similar applications, I noticed few things that play a significant role in this application.

Following are *few* key points to note about this application:

- Privacy and security are key since this application will have to access to several smart devices so in case this application is compromised, then it might let a cyber-criminal to get access to other devices as well, therefore this application will be built in a way that in case its compromised, it will shut down automatically so that cyber-criminal cannot get access to other devices.
- UI of this application is key since the main target audience of this application are the people who might have not enough background in technology or smart devices. So, this application should provide user-friendly UI/UX experience.
- Customer support is key. Since the main purpose application is to provide users a safe way of

The survey was sent to a sample size of 12 who have access to several smart devices including smart mirrors.

accessing smart devices, it's important to have easily accessible customer support in case of security threats or incidents.

A. Survey Questions

As part of the survey, following questions were sent out to users:

1) Do you use strong authentication measures when you're using these smart devices?

2) If you're a smart mirror user, please describe if you have any privacy and security concerns with it.

3) If there's a web/mobile application that can be used to monitor the activity on several smart-devices in your home, would you be interested in using it?

4) If you're interested, could you please your provide your reasons on why you're not interested in using this application?

B. Survey Responses

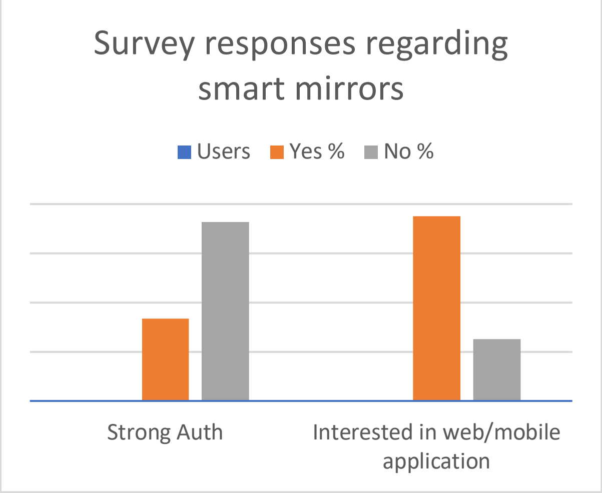

Fig. 1. Survey responses to determine the interest in the proposed application.

Although my sample size for the survey was small, it's important to note that a lot of people are not using strong authentication and they are interested in using an web/mobile application that will help them in monitoring any registered smart devices in their homes.

C. Implementation Process

To implement to the application, I plan to work with few other members such as UI/UX designer, Software Engineer and Security Engineer. I plan to build a mobile-based application first with user-friendly UI/UI along with strong security foundation. I plan to release this feature to certain consumers as part of beta-testing. Based on their review and feedback, I plan to update the application with more features. To allow the users easily access this application, I plan to create several tutorials and include it in the application for users to view and review if necessary.

Once mobile-based application is in a good place, I will start implementing the web-based application and repeat the testing and updating the application process.

In order to implement this application, I plan to use latest web/mobile frameworks such as React, NodeJS, MySQL to create responsive single page applications that can be tested easily. sample size for the survey was small, it's important to note

VI. Evaluation Process of the Application

As part of the evaluation process of the application, I plan to send out few other surveys to evaluate the designs and implementation of the application to understand whether the application would work and if there are key features that this application is lacking. I plan to use one of the rapid, remote testing applications known as Maze to get feedback from users in terms of UI/UX experience while implementing the application in order to provide user-friendly experience.

Since, the main objective of this paper is to propose an application and its implementation process, it's difficult to provide evaluations on how whether the designs and efforts of this application worked at this time. But, I stronly believe that this application will ensure consumer's data is secure and reduce security threats and incidents in the near future by monitoring and educating its users regarding security aspects of the smart devices.

VII. Overview of Relevant Work

The rise in smart devices has slowly enhanced my interest in security aspects of these smart devices. Certain smart devices such as Google Home and its related products provide an easy way of accessing all its products in a single mobile application which allows its consumers to monitor any unauthorized activity or access easily from anywhere. During these unforeseen unfortunate circumstances, I have seen an exponential increase in some other smart devices such as smart mirrors and these smart mirrors increases the risk of data breach due to its data-driven technology. In order to help mitigate these concerns and by taking some inspiration from the Google Home application, I propose to implement a similar application that will allow consumers to register all kinds of smart devices and provide several monitoring services instead of relying on user to manually perform these actions.

Although, I haven't found enough information regarding such applications mainly related to smart mirrors, there are several surveys and reports suggesting that the other applications such as Google Home have reduced the security threats in Google Home devices which proves that this new application will help reduce security threats in other smart devices such as mirrors.

VIII. CONCLUSION

After researching several other similar applications and by using the results from the surveys, the proposed user-friendly application will implemented in a way that will allow its users to register all their smart devices in one place and to be manage easily. It will also provide several monitoring services that will alert in case of any unusual activity instead of users manually performing these tasks. One of the key features of this application is to allow its users shut-down/turn-off any of these smart devices from anywhere using this application or user can set an auto-shutdown task within certain time limits. This application also provides key information on security concerns, potential attacks and preventive measures in order to educate the users.

As part of the implementation process, I plan to use the Maze which is a rapid, remote-testing application which allows us to easily capture feedback before and while implementing the process. Testing and security foundation are the two main key things of this application.

In conclusion, although smart devices are innovative, convenient, easy to use and overall beneficial, there are several security concerns around it. Due to the type of the information that these smart mirrors store or have to access to, they are under huge risk in cyber security community which is why I believe it’s important to educate consumers about the risks and preventive measures to protect user’s privacy and to prevent any security threats.

REFERENCES

[1] Cortne Bonilla, "Are Smart Mirrors Ruining Our Lives?" https://edit.sundayriley.com/are-smart-mirrors-ruining-our-lives/, April 2019.

[2] Lisa Iscrupe, "How hackable are the smart devices in your home? We reveal the most vulnerable homes" https://www.allconnect.com/blog/can-your-smart-home-be-hacked, January 2020

[3] Davey Winder, "Confirmed: 2 Billion Records Exposed In Massive Smart Home Device Breach" https://www.forbes.com/sites/daveywinder/2019/07/02/confirmed-2-billion-records-exposed-in-massive-smart-home-device-breach/?sh=4e5160db411c, July 2019

[4] Emil Sayegh, "Mirror, Mirror on The Wall" https://www.forbes.com/sites/emilsayegh/2021/03/23/mirror-mirror-on-the-wall/?sh=608bea9d4c0d, March 2021

[5] Manasa Reddigari, "The 10 Biggest Security Risks in Today's Smart Home" https://www.bobvila.com/slideshow/the-10-biggest-security-risks-in-today-s-smart-home-53081, February 2020

[6] Teresa Rivas, "Lululemon Is Buying Mirror. Why That’s a Smart Move" https://www.barrons.com/articles/lululemon-is-buying-mirror-why-thats-a-smart-move-51593538863, June 2020

[7] Adam Keesling, "The Future of Fitness" https://every.to/napkin-math/the-future-of-fitness-lululemon-buys-660503, July 2020