Web Application Proposal for Cyber Security Topics, IoT Vulnerabilities, and Password Strength Checker

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Zachery Taylor Morris

Spring, 2017

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature _____ Date _____
Zachery T. Morris

Approved _____ Date _____
Mohammad Mahmoody, Department of Computer Science

Web Application Proposal for Cyber Security Topics, IoT Vulnerabilities, and Password Strength Checker

Zachery Morris
Computer Science
University of Virginia
Charlottesville, Virginia, USA
ztm4qv@virginia.edu

ABSTRACT

The majority of society interacts with the internet of things (IoT) every day without truly understanding the cyber security risks associated with the internet or these devices. A basic knowledge of cyber security and threats related to the IoT would allow people to make better informed decisions about their presence online. To increase people's understanding of potential cyber security threats, the current paper proposes a web application that would combine information regarding three aspects: important cyber security topics, IoT vulnerabilities, and a password strength. Along with the discussion of each cyber security topic, ways for a user to protect themselves and a quiz to check their newly acquired knowledge will be included. Additionally, the IoT vulnerabilities section is broken into two categories: home IoT vulnerabilities and industrial IoT vulnerabilities; both of which, detail ways to mitigate these risks. Lastly, a password strength checker provides insight into the infeasibility for a typed password to be hacked. Every user who explores the web application will gain knowledge in cyber security, and thus, be able to proactively manage their presence in our digital world.

INTRODUCTION

Many analysts suggest that over 50 billion devices will be connected to the internet by the end of 2020 [1]. With these many devices present, the majority of society interacts with the IoT every day, and do not understand the cyber security risks associated with it. IoT allows the communication between electronic devices and sensors through the internet in order to facilitate daily life [2]. IoT is progressively becoming an important aspect of our daily lives, as it connects a variety of smart systems, frameworks, smart devices, and sensors [3]. While the emergence of IoT has progressed society immensely, security of data and information is an important concern and a major challenge. Since the internet is one of the largest sources of security threats and cyber-attacks, hackers have made the data communicated through the internet insecure. The most significant concern of IoT is security and the collaboration between social networks and privacy [3]. Some examples of IoT devices include smart speakers like Amazon Alexa, smartphones, smartwatches, smart home systems, smart appliances, smart health sensing systems, and any device that connects to the internet which transfers data over it.

Despite the risk-reducing impact of good cybersecurity habits and the ever-increasing cyberattacks on business and individuals, a survey conducted by Pew Research Center reveals that out of 1,055 participants, the average respondent answered only 38% of cyber-knowledge questions correctly [4]. Therefore, a basic knowledge of cyber security and threats related to IoT will allow people to make better informed decisions about their presence online. Currently, the only way for a person to gain understanding of cyber security topics, learn about IoT vulnerabilities in the home and industry, and utilize a password strength checker is to find these resources separately. However, there is not a single web application that provides the user with all three functionalities; therefore, suggesting the need for a single resource to provide all three of these, never-before-combined, topics.

To fill this need while increasing individuals' understanding of potential cyber security threats, this paper aims to develop an extensive layout of a web application that combines all three of these topics. This suggests that the web application will not be implemented, but rather, a sufficiently detailed proposal will be provided so the reader understands what is fully being proposed through the application. This application will first describe various aspects of cyber security, followed by ways for someone to protect themselves from IoT vulnerabilities, and ending with a functionality that shows the strength of a user-typed password, therefore, there are three main sections to the website layout. The first section provides information on cyber security topics (malware, privacy, phishing, online scams, data breaches, and public WiFi), how someone can protect themself, and a scenario-based quiz to test their knowledge. The second section highlights IoT vulnerabilities within the home and industry while providing ways to decrease these threats. Lastly, the third section, provides users with a password strength checker that shows if the typed password is weak (can be easily hacked) or strong (is not easily hacked). The last functionality mentioned will better prepare users for creating strong and, potentially, unbreakable passwords. Whereas the first two functionalities provide users knowledge in cyber security, and thus, the ability to proactively manage their presence in our digital world.

RELATED WORK

Like previously stated, there are other websites that discuss only one of the three aspects the proposed web application will contain. There are many websites that provide information on cyber security topics such as a website called, "SearchSecurity" but this is the only function of the website [5]. Similarly, there are many web applications that provide users with a password strength checker, one of the most notable is called: "The Password Meter" [6]. Additionally, most of these sites specialize in one of these three topics, and go into depth on the topic. These websites target audiences that have studied a technical major, like computer science, since the sites delve into the technical concepts or implementations. They do not appeal to a user that has not had much formal technical knowledge. For instance, someone who has studied a non-STEM major or an older generation user, who has limited technical knowledge, will not benefit from these sites since they will not be able to understand the concepts. Furthermore, many of these websites fail to provide users with how the concepts are applicable to the real-world. Instead, the sites provide only information which can lead to a lower retention of information.

One such website is called TechTarget which details multiple cyber security topics like data security, encryption, identity and access management, and software security [5]. This website, however, goes into technical details regarding each topic. For example, for the data security topic, the site speaks about artificial intelligence (AI) and how it can protect against threats. AI is a topic that a normal user, who has minimal technical knowledge, will not understand. Moreover, the site does not provide the user with ways they can protect themselves from the threats in each cyber topic. Rather, the website says how computer scientists can protect the public by implementing certain functionalities through AI. Additionally, TechTarget has a convoluted design in the fact that it is difficult to navigate the web pages in order to find the information a user would need.

In contrast to these websites, the proposed web application in this paper combines all three of these topics to create a cohesive learning environment for someone who is learning about multiple aspects of cyber security. Moreover, the application discusses these topics at a high level in order to appeal to users who have minimal technical experience. In this way, all users will be able to understand the information present, and gain knowledge about cyber security. Not only does the application provide users with concise and easily understandable cyber security concepts, but it also provides users a way to test their newly acquired knowledge. For each cyber security topic, there is a scenario-based quiz that allows a user to choose the most secure route to take. Unlike other resources online, this application allows for users to learn and test their knowledge through real-world applications which increases knowledge retention.

TOOL ARCHITECTURE

This tool is a dynamic web application that consists of multiple diverse, distributed, and dynamically generated web components. These components implement different parts of the application's functionality and interact with each other to provide services to the users. The web application has three functions: information on cyber security topics, information on IoT vulnerabilities, and password strength checker.

1.1 Client-Side Components

The web application has client-side components created by using HTML, CSS, bootstrap, and JS. Each webpage will utilize HTML, CSS, and bootstrap in order to elicit high UX and UI. The webpage that has the password strength checker will include dynamic behavior, client-side input validation, and DOM manipulation using JavaScript to modify the page according to the user's inputted password.

1.2 Server-Side Components

The web application implements state handling in order to support multiple users. Using a server-side $_SESSION object to maintain state of the application on the server allows for multiple users.

SYSTEM DESIGN

2.1 Homepage

The purpose of the homepage welcomes the user to the application and provides an overview of the web application's functionalities.

Figure 1: Wireframe of the web application's homepage

2.2 First Functionality – Information on Cyber Security Topics with Quizzes

The purpose of this functionality is to provide the user with an overview of various cyber security topics that are relevant to someone who is trying to protect themselves from malicious attacks. Additionally, this functionality is meant to test if the user has gained a better cyber security judgement, based on the topic at-hand, by taking a single question scenario-based quiz. The functionality

allows users to view information regarding malware, privacy, data breaches, phishing attacks, online scams, public Wi-Fi which are all detailed in Figure 3 [7]. Moreover, the functionality allows users to participate in a scenario-based quiz, which is meant to provide the user with immediate feedback on their learning of cyber security topics. There is no hard implementation here, rather, the information about each specific topic is presented with the use of HTML, CSS, and bootstrap. The scenario-based quiz is implemented using JavaScript. When the user clicks on the correct answer, the correct answer is highlighted in blue. However, if the user clicks on the incorrect answer, the answer they chose is highlighted in red. The user can expect to see information and examples regarding the specific cyber security topic. Additionally, the user can expect to be able to answer scenario-based questions relevant to the topic at hand.

Figure 2: Wireframe of "Cyber Security Topics" informational functionality

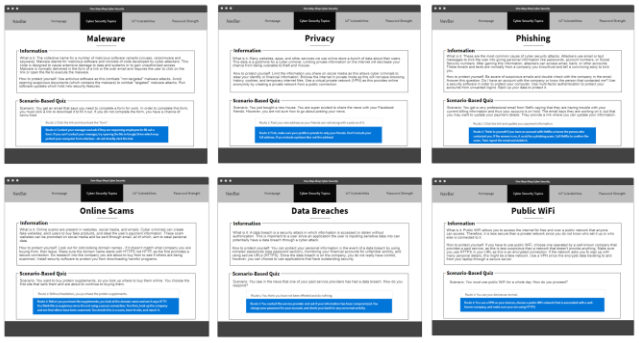

Figure 3: Six wireframes where each details a cyber security topic, how a user can protect themself, and the scenario-based quiz

2.3 Second Functionality – Information on IoT Vulnerabilities

This section of the web application is meant to provide users with information on IoT vulnerabilities that are compartmentalized into two categories: home and industry as seen in Figure 4. This functionality aims to help consumers make informed decisions about purchasing IoT devices and provide knowledge on IoT devices used in industry. Additionally, this functionality aids users in minimizing vulnerabilities associated with IoT devices. The functionality is separated into home IoT vulnerabilities and industry IoT vulnerabilities. Therefore, the user is able to view information on existing vulnerabilities, poor configuration, and the use of default passwords, which are most common among home IoT vulnerabilities. Additionally, information on industrial IoT threats such as man-in-the-middle, device hijacking, distributed denial of service (DDoS), and permanent denial of service (PDoS) will be provided along with countermeasures, such as firmware integrity, mutual authentication, and secure communication as seen in Figure 5 and 6. There is no hard implementation here, rather, the information about each specific topic is presented in web pages with the use of HTML, CSS, and bootstrap. Moreover, the user can expect to see information about and examples of home IoT vulnerabilities and industry IoT vulnerabilities with ways to decrease both which are detailed below.

Figure 4: Wireframe of "IoT Vulnerabilities" informational functionality

2.3.1 Home IoT Vulnerabilities – Information. Each tile in the section "Information" in Figure 5 have information regarding each listed IoT topic. The information listed is detailed below.

2.3.1.1 "Smart Lock/Alarm System". If this IoT device is compromised then cyber attackers have control on who enters or leaves the house. Complex IoT environments (CIE) have multiple IoT devices connected and woven into an environment using an IoT automation platform. Attackers can modify automation rules to have control over the smart lock, and thus, the people who can enter and leave the house [8].

2.3.1.2 "Smart Speaker". If this IoT device is compromised, attackers will be able to make voice commands of their own, which can potentially steal information or activate other connected devices. A potential access point is through open internet ports on the device [8].

2.3.1.3 "Smart Kitchen Devices". IoT devices like smart refrigerators and coffee makers can be hacked by cyber attackers, providing them control of the smart device. These attacks can occur through exploitation of the smart device's internet connection and protocols [8].

2.3.1.4 "Smart Toilet". If this IoT device is compromised, hackers can use the toilet's features to make it flush repeatedly.

These attacks can occur through exploitation of the smart device's Bluetooth connection [8].

2.3.2 Home IoT Vulnerabilities – Ways to Mitigate. Each tile in the section "Ways to Mitigate" in Figure 5 have information regarding each listed topic. The information listed is detailed below.

2.3.1.1 "Map Connected Devices". All of the devices connected to the same network should have their settings, credentials, and firmware versions accounted for. By doing this, a user can know what security measures to take with each device, and discover which devices need to be replaced or updated.

2.3.1.2 "Change Default Passwords". Make sure each device has a unique password besides the ones preset from the manufacturer, so the device is less likely to be hacked [9].

2.3.1.3 "Check Automation Rule Files". Check automation rules to track changes made. This will help to discover if something has been modified, therefore, defending against potential threats [8].

2.3.1.4 "Be Knowledgeable About Settings of each Device". Turn off unnecessary services in order to decrease the data gathered by a device, and make sure the device's server settings are secure.

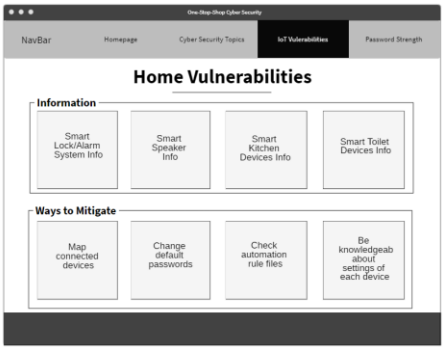

Figure 5: Wireframe of four home IoT vulnerabilities and four ways to mitigate them

2.3.3 Industrial IoT Vulnerabilities – Types of Attacks. Each tile in the section "Types of Attacks", in Figure 6, have information regarding each listed topic. The information listed is detailed below.

2.3.3.1 "Man-In-The-Middle". When an attacker interrupts communication between two devices. As an example, an attacker blocks signal from system to IoT assembly robot arm and makes the robot cause damage within the processing line [10].

2.3.3.2 "Device Hijacking". When an attacker gains control of a device. This is difficult to detect as the attacker leaves the functionality of the device alone. Example: attacker gains control of a smart meter and penetrates malware into the energy systems [10].

2.3.3.3 "Distributed Denial of Service (DDoS)". Temporarily interrupt services of a host connected to the internet in order to make a device unavailable. These attacks can cause major interruptions to services and manufacturing systems [10].

2.3.3.4 "Permanent Denial of Service (PDoS)". When an attacker damages a device to the point where the device can only be replaced. As an example, an application called BrickerBot is used to exploit hard coded passwords in devices. The application causes a PDoS which could be used to damage factory equipment [10].

2.3.4 Industrial IoT Vulnerabilities – Ways to Mitigate. Each tile in the section "Ways to Mitigate", in Figure 6, have information regarding each listed topic. The information listed is detailed below.

2.3.4.1 "Firmware Integrity". Make sure that IoT devices only communicate with authorized services to decrease the probability of downloading malicious programs instead of firmware.

2.3.4.2 "Mutual Authentication". Every IoT device should be authenticated prior to transmitting or receiving data. This step makes sure data collected is from a non-fraudulent source. In other words, both device and service must provide their identity to each other before continuing to transmit data.

2.3.4.3 "Secure Communication". Make sure the data in transit between a service and its device is encrypted. This makes sure the data communicated is unable to be seen by attackers.

2.3.4.4 "Security Monitoring". When data (endpoint devices and connectivity traffic) is collected on the state of a system. This data is then analyzed for security violations. If a threat is detected, then the system's security policy is executed.

Figure 6: Wireframe of four types of IoT attacks and four ways to mitigate them

2.4 Third Functionality – Password Strength Checker

The purpose of this functionality is to provide the users with a way to check the strength of a password. Allowing a user to type and, in real time, update the progress stars to show the strength of the password. This functionality will help with the user's ability to create strong passwords as they can continuously update their previous password to see if another star becomes filled, until all five stars are filled. The functionality updates the progress stars to show how hard it would be to crack the user-typed password. In other words, before the user types anything into the input box, no stars are filled. However, as a user types a password in the input box, the stars fill from left to right. As the password becomes more

complex, the more stars are filled where five stars filled is the maximum.

2.4.1 Implementation. This functionality is implemented using HTML, CSS, and JavaScript. The HTML builds the layout of the page. It displays the title, background information, the text box, and the five stars. CSS styles the content of the page. JavaScript is what displays the filled stars based on what the user enters in the text box. Every time a user enters a new character, the JavaScript code pulls the text, checks its contents, and then displays the correct amount of filled stars.

2.4.1.1 Password Aspects. There are five aspects of a password used by the program to determine if the password is one, two, three, four, or five stars. The first is password length. If the user's password is less than four characters long, the password will gain a score of 5 points. If between five to ten characters, the password will gain 10 points. If twelve or more characters, the password will gain 20 points. The second aspect of the password is alphabetic characters. If there are none, the password will gain 0 points. If they are lowercase letters, the password will gain 10 points. If there is a mix of upper and lower case, the password will gain 20 points. The third aspect of the password is numeric characters. If there are no numbers, the password gains 0 points. If there is one or two, the password gains 10 points. If there are three or more, the password gains 20 points. The fourth aspect of the password is special characters (!, @, #, ?). If there are none, then the password gains 0 points. If there is one, the password gains 10 points. If there is more than one, the password gains 20 points. The fifth aspect of a password is a mix of the previous aspects. If there are letters and numbers, the password gains 2 points. If there are letters, numbers, and special characters, the password gains 3 points. If there are lowercase letters, uppercase letters, numbers, and special characters, the password gains 5 points. This scoring guideline was adopted by cross checking popular password strength checkers like the one present in The Password Checker [6].

2.4.1.2 Star Buckets. After the program analyzes the password and adds together the points gained, the password and its associated score will fall into a specific bucket: zero stars, one star, two stars, three stars, four stars, and five stars. If the password's total score is zero (meaning the user did not enter anything), then zero filled stars are displayed. If the password's total score is greater than 0 and less than or equal to 25, then one filled star is displayed. If the password's total score is greater than 25 and less than or equal to 50, then two filled stars are displayed. If the password's total score is greater than 50 and less than or equal to 70, then three filled stars are displayed. If the password's total score is greater than 70 and less than or equal to 80, then four filled stars are displayed. If the password's total score is greater than 80, then five filled stars are displayed. This range guideline was adopted from Hive Systems' chart on password aspect importance, where they cover each password aspect mentioned and how it relates to password strength [11].

The users can expect to see the progress stars to fill-in based on the aspects of the typed password. As the user deletes parts of the password or adds to the password, the user can expect that the stars will fill and un-fill. The user can expect that the entered password will not be saved in any way.

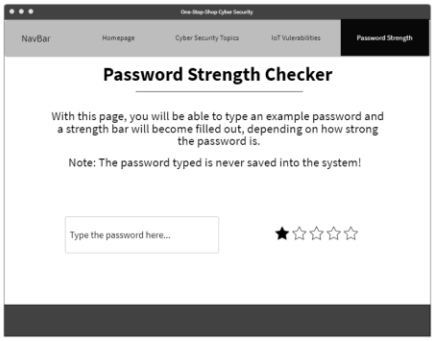

Figure 7: Wireframe of the password strength checker functionality

PROCEDURE

The user will access the site by using the specified URL. Once on the site, the user will see the homepage, as seen in Figure 1, where the user is welcomed to the application and can navigate to the "Cyber Security Topics", "IoT Vulnerabilities", or "Password Strength" pages by clicking on each respective section in the navbar. Then, users navigate to the "Cyber Security Topics" webpage, seen in Figure 2, by clicking the corresponding section in the navbar. On this page, a user sees six different cyber security topics. The user can then choose to learn more about one of the topics by clicking on its box. This will then redirect them to that topic's page, seen in Figure 3, which will detail information regarding the topic, how to protect themselves, and the scenario quiz. Additionally, the quiz section of this functionality is used by reading the scenario related to the cyber topic, and choosing the best route to take based on the information previously read about the cyber security topic. Next, the user clicks the IoT vulnerabilities section of the navbar, and is redirected to a page where they can choose to click "Home IoT Vulnerabilities" or "Industry IoT Vulnerabilities", seen in Figure 4. After clicking on the home choice, the user is redirected to a page that displays information on specific home IoT vulnerabilities, seen in Figure 5, and on how to protect themselves from the threats. Similarly, after clicking on the industry choice, the user is redirected to a page that displays types of attacks heavily made to industry IoT devices and ways to mitigate them, seen in Figure 6. Lastly, a user can navigate to the last functionality by clicking the "Password Checker" section of the navbar. They are redirected to the page, seen in Figure 7, where the user can click into the input box that says "Type the password here…", then they are able to type a password. While they are typing the password, the user can watch the stars fill-in based on the content of the password.

RESULTS

The system solves the issue of seamlessly and effectively providing users with information on different cyber security topics. Unlike other websites, this proposed web application combines information regarding cyber security topics, IoT vulnerabilities, and password strength to provide the user with an easy-to-understand overview of security issues in the digital world.

A third-year student at the University of Virginia, and the roommate of the author, "tested" the system. Since the system is not implemented, the student read through the web application proposal. This student commented that the web application effectively provided a concise overview of security topics. The user detailed that the application reduces the time it takes for users to find security related information online. By combining all three aspects of online security, it allows users to focus more on retaining the information, rather than wasting time to find said information. Additionally, the third-year student is studying computer science and has former knowledge in cyber security. With this background, the user detailed that the application provided them with new information, they previously were unaware of. This suggests that not only will users, who are not technical, benefit from the functionalities present in the application, but users who have a technical background will also benefit due to the applications breadth of cyber security concepts.

CONCLUSION

People who are unaware of cyber security topics, IoT vulnerabilities, and how to create strong passwords would benefit from using this tool. This group of people contains different demographics. For example, older people who are less technologically savvy would want to use this tool so that they have one place where they can learn about cyber security topics, IoT vulnerabilities, and making strong passwords. Additionally, those that are younger would also want to use this tool since they are more likely to interact with internet connect devices, and thus, more prone to vulnerability.

This tool acts as a "one-stop-shop" for popular cyber security topics in order to prepare users for defense against attacks and vulnerabilities. This tool combines many things that can help someone manage their presence online and have control over their vulnerability to attackers. This tool provides different aspects: like information regarding cyber security topics, information about IoT vulnerabilities, and a function that shows password strength. Combining all of these aspects into one tool, would help someone who is new to cyber security topics and does not know where to start. This application provides a starting basis by helping the user gain a better insight into how to protect themselves in the digital world. Specifically, the password strength checker is beneficial if a different website asks for the user to create a password and does not show the user how strong of a password it is. With this tool's functionality, the user would be able to enter a possible password and the screen updates in real-time to show the strength of said password.

FUTURE WORK

As stated previously, the system currently has no implementation as only an extensive proposal is provided. Therefore, future work needs to be done to implement the web application. Additionally, the web application's sections on cyber security topics and IoT vulnerabilities could be expanded to provide users with even more information in the security realm. For example, the cyber security section could detail additional topics like firewalls and mobile security. Moreover, the scenario-based quizzes in the cyber security topics section could be implemented in the IoT vulnerabilities section as this would provide users with more connections to the real-world. Lastly, the password checker functionality can be expanded to determine password strength, not only by brute force cracking, but also, by dictionary cracking.

If the system could support all the above additions, it could possibly rival even the most popular cyber security information sites, and even take users away from using such sites as it provides similar services, but in a comprehensive and modern interface.

REFERENCES

[1] C. Maple, "Security and privacy in the internet of things," Journal of Cyber Policy, vol. 2, no. 2, pp. 155–184, 2017.

[2] M. Silverio-Fernández, S. Renukappa, and S. Suresh, "What is a smart device? - a conceptualization within the paradigm of the internet of things," Visualization in Engineering, vol. 6, no. 1, May 2018.

[3] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," *Journal of Big Data*, vol. 6, no. 1, Dec. 2019.

[4] Pew Research Center, "What the Public Knows About Cybersecurity," *Pew Research Center*, 2017. [Online]. Available: https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/ [Accessed Oct. 23, 2020].

[5] "Information Security Topics - SearchSecurity," TechTarget. [Online]. Available: https://searchsecurity.techtarget.com/resources. [Accessed: 23-Oct-2020].

[6] "The Password Meter," Password Strength Checker. [Online]. Available: http://www.passwordmeter.com/. [Accessed: 23-Oct-2020].

[7] "7 Of The Most Important Cyber Security Topics You Should Learn About," Norton, 26-Apr-2019. [Online]. Available: https://us.norton.com/internetsecurity-how-to-7-most-important-cyber-security-topics-you-should-learn-about.html. [Accessed: 23-Oct-2020].

[8] Z. Chang, "Inside the Smart Home: IoT Device Threats and Attack Scenarios," Trend Micro, 30-Jul-2019. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios. [Accessed: 23-Oct-2020].

[9] J. Ellis, "What Makes A Strong Password?," SandStorm IT, 14-Oct-2019. [Online]. Available: https://sandstormit.com/what-makes-a-strong-password/. [Accessed: 23-Oct-2020].

[10] "Industrial IoT: Threats and Countermeasures," Rambus. [Online]. Available: https://www.rambus.com/iot/industrial-iot/. [Accessed: 23-Oct-2020].

[11] "Are Your Passwords in the Green?," Hive Systems, 19-Aug-2020. [Online]. Available: https://www.hivesystems.io/blog/are-your-passwords-in-the-green. [Accessed: 23-Oct-2020].