Group Ideation

Authors redacted

1) Blindfold: A Mechanical Cover for a Smart Device to Reduce Bystanders' Concern on the Use of Camera Devices in Public Spaces

Contribution

Video/photo shooting using a smart device without any permission in a public area has caused a privacy issue internationally. However, there is not much work done regarding this topic. By developing a simple mechanically controllable shutter for the device's camera lens, we would like to collect data about usability of the shutter and how effective the shutter is in terms of how much of bystanders' privacy concern can be mitigated.

Motivation

As the number of smart devices increases, the number of cameras deployed around a user increases. This would be able to cause a serious privacy invasion once a hacker gets access to using the user's camera. [1] Even though some users cover their laptop's or smartphone's camera with a tape, many users have not been aware of the potential consequence caused by the vulnerability of the camera access. In addition, governments in Korea and Japan regulated the law that smartphones should generate a camera shutter sound when a user takes a photo with a smartphone to prevent the potential crime to record someone without permission. For these problems, a robotic cover for a smart device camera can be used to reduce privacy concerns of a user by blocking vision of the camera so that the cover can be open only when a user wants to use it.

Implementation

We are building a smartphone case that has a mechanically controllable shutter for its camera lens. For example, if a user is using a camera, the shutter opens and the camera lens is exposed outside, and if not, the shutter closes the lens. Currently, we plan to make a plug-and-play smartphone case for an Android device (Samsung Galaxy 4) such that when a user covers their smartphone with the case, the shutter can be automatically activated.

Study Methods

As an initial step, we plan to conduct two types of lab studies to examine (1) the usability of the system and (2) how effective the shutter is in terms of how much of bystanders' privacy concern can be mitigated. We plan to recruit 5 participants who have experiences using a smartphone for each study.

The first study is conducted individually. A researcher provides a participant with a device that has our Blindfold device set up. Then, a researcher asks them to do three rounds of 5 tasks in random order: (1) sending a text message (2) using a social media service (3) video shooting (4) taking a photo (5) turning on/off a phone. After three rounds, the participant is asked to rank the usability of the technology using the 10 Likert questions from the System Usability Scale (SUS) adopted from the questionnaire design of De Cristofaro, E. et al. [3]. 10 question categories are as follows: convenient, quick, enjoyable, reusable, helpful, user friendly, easy, stressful, trustworthy, secure. From this study, we can collect the results and reflect on this for a better system design.

The second study is also conducted individually. However, for this study, in the first session, a researcher is using a smartphone device without the Blindfold device and a participant is asked to watch the researcher using it. In the second session, the researcher is using the Blindfold device and a participant is asked to watch the researcher using it. While the researcher is working on tasks (same as the first study), the participant is asked to watch the behavior for three minutes. After two sessions, the participant is asked to answer questions on a questionnaire the researcher provides. The questions are as follows: (1) did you feel the counterpart tried to take a photo or recorded a video of you? (2) If so, how many times did you think the counterpart takes a photo/video of you. (3) did you feel the counterpart invaded your privacy? Each question has Likert scale with 5 options: strongly agree, agree, normal, disagree, strongly disagree. After the data collection, we can reflect the result and examine the impact on a user's privacy concern.

References

[1]https://www.theguardian.com/commentisfree/2018/apr/06/phone-camera-microphone-spying

[2] https://www.techdirt.com/articles/20031111/099242.shtml

[3] De Cristofaro, E., Du, H., Freudiger, J., and Norcie, G. A comparative usability study of two-factor authentication. In Proceedings of the Workshop on Usable Security (USEC) (2014).

2) Haptic Feedback User Study for Spidey Sense

Contribution

Despite the importance of a user's security management, people are often not motivated since they do not feel unsafe the same way they might if they were walking down a dark alleyway alone at night. The research goal with Spidey Sense is to develop a novel tool to communicate important cybersecurity risks to users at a visceral level. As a part of this project, we will conduct a study to see how creepy-crawly sensations can be naturally mapped to a human's perception, of which the results will be a key component of the future Spidey Sense system design.

Implementation

By leveraging the fact that many people started wearing a smartwatch, we decided to design a replaceable smartwatch band such that a user can easily set up the Spidey Sense system on their smartwatch. The Spidey Sense smartwatch band has a robot-finger-looking actuator that provides various sensation types to a user. The robot finger actuator is designed to touch and scratch a user's wrist by moving back and forth. By varying the level of actuation pressure, this finger can provide tickling, creepy-crawly, and scratch sensation types. From a user study, we want to see the natural mapping between the haptic feedback types and a user's emotional perception about each type of haptic feedback.

Study Method

We can set up a lab study environment and recruit around 20 participants who experience wearing a smartwatch. The study will be conducted individually in a quiet area to remove other potential factors to affect the study's result. Once a participant is ready, a researcher provides a smartwatch that has a Spidey Sense smartwatch band. Then, a researcher provides haptic feedback (tickling/creepy-crawly/scratch) from the band remotely. Each participant receives the haptic feedback 20 times in a random order. Only one feedback type is provided per round. At the same time, the participant needs to choose their emotional perception every round from a questionnaire on a computer the researcher provides. The questionnaire has 5 options: 1) nothing 2) pleasant 3) creepy 4) annoying 5) I don't know. After 20 rounds of experiments, a participant can return the device and leave. Researchers will collect data and provide analysis about the result.

References

[1] Graham Wilson, Harry Maxwell, and Mike Just. 2017. Everything's Cool: Extending Security Warnings with Thermal Feedback. In Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '17). ACM, New York, NY, USA, 2232-2239.

[2] Marc Teyssier, Gilles Bailly, Catherine Pelachaud, and Eric Lecolinet. 2018. MobiLimb: Augmenting Mobile Devices with a Robotic Limb. In Proceedings of the 31st Annual ACM Symposium on User Interface Software and Technology (UIST '18). ACM, New York, NY, USA, 53-63.

3) User Study for TablePathy: Acoustic-based Short-distance Wireless Communication Technique for Secure Data Transfer

Contribution

TablePathy is a novel system that enables devices placed on the same physical media (e.g., a table) to wirelessly communicate securely for the following target directions: (1) a system to prevent the man in the middle attack [1,2,3,4] (2) automatic authentication between multiple devices (3) secure communication for a local group of users. One of the important parts to designing this system is about usability. From this project, we plan to conduct a user study to examine the system's usability.

Implementation

We are using two smartphones (Phone A, Phone B) and an office table (located in TSRB lab 243) for preliminary tests. The key point of this technique is that two smartphones can communicate by sound propagated through a physical media (the office table) and this sound should not be received by a device not placed on the table. In order to avoid this case, we are currently testing which sound can be transferred well through the table but not received well by the device that does not have physical contact with the table. Signal processing techniques are utilized to examine which frequency components of the sound have such a property. Finding the meaningful parameters is also important. As an initial step, we set the following parameters to see the effect of each variable on the system performance: (1) distance between devices (2) gap between a table and a device (3) volume of a sender device. After finding “good” sounds that exhibit a desired performance, we are planning to build applications.

Study Methods

From this project, we are focusing our goal on examining the system’s usability. To do that, we plan to do a lab study. Specifically, we recruit 10 people who have more than one electronic device that requires any types of authentication. Our researcher shows three different scenarios that the TablePathy system is designed to target for, and teaches the participants the basic concept and how to use it. After the instruction, we ask them to use the technology in the aforementioned three cases. The study consists of three rounds, and from each round, the researcher asks the participant to use the system for one case. After each round, the participant is asked to rank the usability of the technology using the 10 Likert questions from the System Usability Scale (SUS) adopted from the questionnaire design of De Cristofaro, E. et al. [5]. 10 question categories are as follows: convenient, quick, enjoyable, reusable, helpful, user friendly, easy, stressful, trustworthy, secure. From this study, we can collect the result and reflect this for designing the better system design.

References

[1] Lonzetta, A.M.; Cope, P.; Campbell, J.; Mohd, B.J.; Hayajneh, T. Security Vulnerabilities in Bluetooth Technology as Used in IoT. J. Sens. Actuator Netw. 2018, 7, 28.

[2] M. Conti, N. Dragoni and V. Lesyk, "A Survey of Man In The Middle Attacks," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027-2051, third quarter 2016.

[3] N. A. Chattha, "NFC — Vulnerabilities and defense," 2014 Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, 2014, pp. 35-38.

[4] M. M. Hossain, M. Fotouhi and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," 2015 IEEE World Congress on Services, New York, NY, 2015, pp. 21-28.

[5] De Cristofaro, E., Du, H., Freudiger, J., and Norcie, G. A comparative usability study of two-factor authentication. In Proceedings of the Workshop on Usable Security (USEC) (2014).

[6] Dianqi Han, Yimin Chen, Tao Li, Rui Zhang, Yaochao Zhang, and Terri Hedgpeth. 2018. Proximity-Proof: Secure and Usable Mobile Two-Factor Authentication. In Proceedings of the 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18). ACM, New York, NY, USA, 401-415. DOI: https://doi.org/10.1145/3241539.3241574

[7] I. Hwang, J. Cho and S. Oh, "Privacy-Aware Communication for Smartphones Using Vibration," 2012 IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, Seoul, 2012, pp. 447-452. doi: 10.1109/RTCSA.2012.43
[8] Nikolaos Karapanos, Claudio Marforio, Claudio Soriente, and Srdjan Čapkun. 2015. Sound-proof: usable two-factor authentication based on ambient sound. In Proceedings of the 24th USENIX Conference on Security Symposium (SEC'15), Jaeyeon Jung (Ed.). USENIX Association, Berkeley, CA, USA, 483-498.

4) Vi Any Means: Using vibration code of a smartwatch and vibration dampening analysis to authenticate devices without using biometrics

Contribution

Biometric information has been used as one of the most secured methods for an authentication system. However, this biometric-based security system shows its vulnerability in various ways [1]. Our proposed method can propose an usable and safe way to authenticate by using a smartwatch vibration functionality and an individual arm's unique vibration dampening characteristic, which can replace the biometric-based system. First, each smartwatch has its unique vibration code (like morse code), which can be a first step login. Second, a user's skin vibration dampening feature is analyzed as a second factor for the authentication. Then, for example, even if a stranger wears a user's smartwatch, the stranger cannot authenticate the user's device since the stranger's skin vibration dampening property is different from the user's. [3, 4] The contribution of this work is three-fold: (1) Novel usable two factor authentication system implementation (2) Secured way to authenticate over a biometric-based authentication system (3) a novel approach to building an authentication system using a vibration dampening property.

Implementation

We are planning to use an Android OS smartwatch or an Apple Watch for the first prototype. Also, we are going to attach the MPU-6050 sensor [2] to a target device we want to authenticate with the smartwatch. This sensor can detect the vibration at 1kHz sampling rate, which can detect relatively accurately not just vibration code provided by the smartwatch but also dampening level caused by an individual's skin characteristic.

The whole scenario is as follows. First, a user wears a smartwatch and activates their secret vibration code. Second, the user touches a target device the user wants to authenticate. Then, the target device analyzes whether it is the right secret code or not and the vibration dampening level. Lastly, if it is the right user, the target device can be authenticated.

Study Methods

In our study, we plan to focus our goal on examining the usability of the system and the performance accuracy. We would like to recruit 10 participants and conduct a user study individually. The study consists of three sessions: (1) a session for training a user's data (2) a session to test the system (3) Survey about the usability.

In the first session, a participant is asked to wear a smartwatch. Then, a researcher provides a smartphone with the MPU-6050 sensor attached to the phone. First, the researcher activates a smartwatch's secret vibration code remotely. Whenever it is activated, the participant holds the phone so that the phone can detect the vibration. Data collection will be conducted 20 times for each participant. After data collection from all the participants, the researcher trains the data and implements the authentication system on the phone.

In the second session, the basic setup is the same as the first session. However, for this time, the phone is ready to be authenticated. A participant is asked to hold the phone and the researcher activates the secret vibration code. Then, we expect the device to differentiate and authenticate the user. In the meantime, the researcher records the accuracy of the authentication.

Lastly, each participant is asked to answer questions about usability of the system. All the questions have one Likert scale and an open-ended question. Since we want to examine the advantages of this system over biometric-based systems, all the questions contain the content regarding the comparison with biometric-based systems: (1) Do you feel this system is safer than biometric-based authentication systems? Why? (2) Do you feel this system is easier to use than biometric-based authentication systems? Why? (3) Do you want to reuse this system over biometric-based authentication systems? Why? After the survey, we plan to reflect the result on our design to improve the system.

References

[1] M. Faundez-Zanuy, "On the vulnerability of biometric security systems," in IEEE Aerospace and Electronic Systems Magazine, vol. 19, no. 6, pp. 3-8, June 2004.

[2] https://playground.arduino.cc/Main/MPU-6050#easy

[3] Marcus ANDERSSON Johan Gustafsson Martin Evert Gustaf Hillbratt Tobias Good (2018), UNITED STATES OF AMERICA Patent No. US20180376261A1

[4] Sungjae Hwang, Andrea Bianchi, and Kwang-yun Wohn. 2013. VibPress: estimating pressure input using vibration absorption on mobile devices. In Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services (MobileHCI '13). ACM, New York

5) Comprehensive study of dedicated 2FA applications

There have been studies on the function and usability of 2FA solutions. However, this usually spans between SMS one-time codes, a physical token, or a dedicated app. This study focuses on the idea that push notifications and one-time codes in a dedicated application is becoming more generally used than the other two. With this in mind, we would look at a comprehensive list of apps (e.g.: Google Authenticator, Duo Mobile, Microsoft Authenticator, LastPass Authenticator, and many more) in order to determine what aspects users find easily intuitive in terms of the setup and authentication process. The research project would be to individually analyze the usability of the applications and identify aspects in the apps that create a more efficient experience for the end user. Surveys would initially ask how users would prefer the system to work and then go into examples with screenshots to ask how they may think of the design. Next a participant study of less than 20 people could be done where they have time to physically use each individual app and do the set-up process in order to see which one seems most function to the end user.

References

[1] Nancy Gunson; "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking" https://www.sciencedirect.com/science/article/pii/S0167404810001148
[2] https://arxiv.org/pdf/1309.5344.pdf

6) Privacy Clippy: Privacy Explaining Browser Extension

Many users are aware their website visits are used to formulate targeted ads or either identifying details about themselves, but they may not necessarily know what that means or how to prevent this. The idea behind Privacy Clippy is to create an educational browser extension that helps explain and educate aspects used to uniquely identify devices and prevent that tracking. Many applications have this ability to stop tracking and ads, but there is not a learning tool that would teach someone what the significance of those items are. This tool would learn from the user and only give relevant advice and recommendations based on the calculated skill level of the user. A user study could be done to help understand if the target audience would use it and learn from the extension as well [1].

References

[1] Y. Wang, P. Leon, A. Acquisiti, L. Cranor, A. Forget, N. Sadeh. A field trial of privacy nudges on facebook. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'14) https://dl.acm.org/citation.cfm?id=2556288.2557413.

7) Shareable Password System Design Jam

Contribution

In today's world, socially connected individuals share secure information such as passwords to accounts [5] and PIN numbers to banking accounts[4]. While sharing this information can be risky and dangerous, people still engage in these behaviors. Thumprint [3] is one existing study that uses a specific pattern input to authenticate users for shared accounts. This study focuses on the technical feasibility and human ability to replicate these knocks. In our study, we aim to explore secure alternative methods of sharing secure or private information like passwords and credentials for shared accounts like Netflix or Wifi. This project will make the following contributions: 1) Determine what systems people would actually want to use to increase efficiency while preserving security integrity when sharing secure information. 2) Produce answers as to why certain ideas and systems are not as popular as others. 3) Develop ideas to implement in further research.

Method

We will start with a design jam approach [1][2] where we conduct focus groups with 15 participants each for 2 sessions. These sessions will last around 30 minutes to an hour. We will use the prompt of designing a system to access a shared piece of information, such as a password or PIN number, to initiate idea generation. Researchers will be taking notes and recording the sessions. We will then have breakout sessions with 5 participants per group with researchers also partaking in the design activity to help facilitate. These groups will further refine the idea of their choice. We will come back as a group to assess the ideas on a creativity – feasibility scale.

References

[1]https://medium.com/ucimhcid/how-to-run-a-design-jam-b3c0f416cb2e
[2]https://www.si.umich.edu/icareers/employers/how-create-campus-presence/campus-recruiting/design-jams
[3]S Das, G. Laput, C. Harrison and J. Hong. Thumprint: Socially-Inclusive Local Group Authentication Through Shared Secret Knocks. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI'17).
[4] S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink, M. Furlong (2007) Security Design Based on Social and Cultural Practice: Sharing of Passwords. In: Aykin N. (eds) Usability and Internationalization. Global and Local User Interfaces. UI-HCII 2007. Lecture Notes in Computer Science, vol 4560. Springer, Berlin, Heidelberg
[5] M. Whitty, J. Doodson, S. Creese, D. HodgesIndividual differences in cyber security behaviors: an examination of who is sharing passwords Cyberpsychol Behav Soc Netw, 18 (1) (2015), pp. 3-7

8) Evaluation of Thumprint

Contribution

Our study aims to extend the Thumprint [2] study to determine how usable Thumprint actually is by conducting usability tests and evaluations on the system. By assessing the system in this manner we not only determine if Thumprint is easily usable but also find where the system can be improved upon. Our goal is to improve the usability of Thumprint for everyday users while maintaining the security of the system.

Method

We will conduct 15 - 30 usability test sessions asking participants to go through specific predefined tasks. At the end of the tasks, we will ask participants questions from the SUS [1] to determine overall usability of Thumprint. In tandem with the usability test sessions, we will evaluate Thumprint by conducting cognitive walkthroughs [3] and heuristic evaluations [4]. Data collected will be used to discuss how the next iteration of Thumprint can be improved upon in terms of usability and design.

References

[1] https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html
[2] S Das, G. Laput, C. Harrison and J. Hong. Thumprint: Socially-Inclusive Local Group Authentication Through Shared Secret Knocks. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI'17).
[3] Cathleen Wharton, John Rieman, Clayton Lewis, and Peter Polson. 1994. The cognitive walkthrough method: a practitioner's guide. In Usability inspection methods, Jakob Nielsen and Robert L. Mack (Eds.). John Wiley & Sons, Inc., New York, NY, USA 105-140.
[4] https://www.nngroup.com/articles/ten-usability-heuristics/

9) Security & Privacy Games for Children

Contribution

The goal of this project is to create and implement an educational game for children to help develop cybersecurity and privacy behaviors. Mobile games have been seen to have a positive effect on privacy & security awareness [1][2][3]. By incorporating this knowledge into children's education, we aim to bring awareness at an early age and foster lifelong techniques for privacy & security.

Method

There are two ways that this can be accomplished: 1) we develop a game and have children evaluate using usability testing, 2) we interview children about their gaming choices and habits and develop the game using data collected from these interviews to inform our design and development.

[1] Alotaibi, F., Furnell, S., Stengel, I., Papadaki, M.: A review of using gaming technology for cyber-security awareness. Int. J. Inf. Secur. Res. (IJISR) 6(2), 660–666 (2016)
[2]http://infonomics-society.org/wp-content/uploads/jitst/published-papers/volume-6-2018/Design-and-Evaluation-of-Mobile-Games-for-Enhancing-Cyber-Security-Awareness.pdf
[3] http://nectar.northampton.ac.uk/8279/1/Hendrix20168279.pdf

10) Privacy & Security Games for Adults

Contribution

This is very similar to the previous idea, except we would be designing a game that teaches adults better security and privacy practices. Alotaibi et al already developed two games for password and malware awareness [2] and evaluated them. Our goal would be to develop an interactive game that teaches the basic fundamental security and privacy practices that adults should be using while also using ambient notifications to help them implement improved changes to their current cybersecurity. We aim to not only educate but also determine if this method facilitates behavioral changes over long term use.

Method

We would conduct user interviews with 15-30 participants about their privacy & security knowledge and practices using the SEBIS questionnaire [4]. During these interviews we would use a semi-structured interview to determine current problems and issues they face with privacy & security based on the fundamental practices that all people should be doing. Another aim of the interview would be to learn about their current gaming habits and preferences. We would then design and prototype a game based on the data collected that would use an incremental approach to help improve people's cybersecurity behaviors. While the ultimate goal would be to do a user study over a long period of time and then reassess using the SEBIS questionnaire to determine behavioral changes, this will not be doable in the short time frame given. Thus the primary goal of the project would be the game development.

References

[1] Alotaibi, F., Furnell, S., Stengel, I., Papadaki, M.: A review of using gaming technology for cyber-security awareness. Int. J. Inf. Secur. Res. (IJISR) 6(2), 660–666 (2016)

[2]http://infonomics-society.org/wp-content/uploads/jitst/published-papers/volume-6-2018/Design-and-Evaluation-of-Mobile-Games-for-Enhancing-Cyber-Security-Awareness.pdf

[3] http://nectar.northampton.ac.uk/8279/1/Hendrix20168279.pdf

[4] Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15). ACM, New York, NY, USA, 2873-2882. DOI: https://doi.org/10.1145/2702123.2702249

11) Stewarded IoT Management

The emergence of wearables and the Internet of Things (IoT) in recent years has already introduced complex security challenges. Hackers and criminals have been exploiting the inferior security of these new devices as vulnerable points of entry into a network. While enterprises are benefiting from product offerings geared towards IoT security, home networks are becoming more and more vulnerable to attacks via thermostats, light bulbs, refrigerators, and other appliances connected to the web. We would like to develop an asset management platform for the home, which would maintain a dynamic inventory of all internet-connected devices on a given network. An initial scan would isolate any active IP address and identify any ports in use. Users would then confirm that each populated record is indeed one of their devices and approve each one. Once a device is approved and added to the user's inventory list, it becomes supervised, so that its settings are evaluated and its software is continually monitored for updates. If a device is found to be vulnerable due to an outdated software version or weak security settings, the user is notified and prompted to take an appropriate action. Ideally, our platform would be able to provide software updates and modify security settings without requiring users to leave the application; however, the first iteration would likely only provide step-by-step instructions on how to set automatic updates or modify relevant settings.

References

[1] https://www.interpol.int/News-and-media/News/2018/N2018-007
[2] Z. Zhang, M. C. Cho, C. Wang, C. Hsu, C. Chen and S. Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications (SOCA), Matsue, Japan, 2014, pp. 230-234. doi:10.1109/SOCA.2014.58

12) Family MDM

As more and more consumer products become connected to the internet, smartphones—being the new center of control—will gain access to even more data. There are several enterprise solutions on the market for mobile device management (MDM) and unified endpoint management (UEM), such as VMware's Workspace ONE. However, there is nothing remotely similar for the consumer market. Most families or households tend to rely on a single relative for their customer support needs. Given this dynamic, we seek to develop a simplified MDM platform for family (or individual) use, so that tech-savvy users can easily supervise and troubleshoot devices, whether it is their own or their grandparents'.

References

[1]https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/mobile-device-management-a-risk-discussion-for-it-decision.cfm

13) Network Vulnerability Scanner for Novices

There are plenty of enterprise and consumer grade network scanners available on the market, but every single one has been developed with professionals or tech-savvy users in mind. Instead, we would like to develop an easy-to-use barebones alternative for the average internet user. Rather than provide dozens of different scanning and analytics capabilities, this tool would have a single option to scan the entire network to which the device is connected to. The results would be populated in a much simplified manner, so that users are presented easy-to-understand, actionable steps they can take in just minutes to address whatever security concerns are identified. Then, as the user becomes more familiar with basic network functionality, additional settings and options will be unlocked. Thus, users would gradually be introduced to security and privacy concepts and become more aware of the risks stemming from their online behavior.

References

[1] Users are not the enemy

14) Analytics tool for Understanding Privacy Policies

Privacy Policies are an essential way for companies to inform their user's what they are with regards to user data and other information the company may obtain. Unfortunately, many privacy policies are written in legal language that make it difficult to understand. The average American has a reading level between 7th and 8th grade [1]. The Kincaid-Flesch Reading ease score is used to analyze a document and give the necessary grade reading level required to understand the material. A study by Common Sense media has shown that most privacy policies fall within the 10th grade range. An idea would be to create a website that analyzes privacy policies using text analytics and gives a summary to users what the main parts of the policy are stating. The system would allow a user to put in a website linking to the privacy policy and the tool would analyze the document if it hasn't already done so and give those conclusions [2].

References

[1]https://www.commonsense.org/education/blog/its-not-you-privacy-policies-are-difficult-to-read

[2] G. Karjoth and M. Schunter, "A privacy policy model for enterprises," Proceedings 15th IEEE Computer Security Foundations Workshop. CSFW-15, Cape Breton, NS, Canada, 2002, pp. 271-281.doi: 10.1109/CSFW.2002.1021821keywords: {data privacy;authorisation;privacy policy model;enterprises;technical mechanism;flexible authorization framework;grantors;obligations;privacy control language;Data privacy;Access control;Authorization;Data security;Protection;Information security;Laboratories;Large-scale systems;Electronic commerce;Natural languages}, URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1021821&isnumber=21985

15) Car Security Application

Car locks and alarms have improved as technology has evolved. Yet, in 2017 over 770,000 cars were reported stolen in the United States [1]. Since this is still an ongoing problem there have been some solutions to allowing the car owners to know when their car is being moved. Using the on-board diagnostics (OBDII) port that is standard in all cars sold in the U.S. after 1996, you can get a lot of information about the car including engine codes, battery voltage, and other useful tools to mechanics [2]. However, the port can also be used to have a permanent tracker in the car that reports when a car is moved out of a specified geo-fence. Unfortunately, most of the technology only exists in tracking and is through a website. Bringing this idea in 2019, you can use the same technology and code the OBDII device to work with a dedicated application that has a subscription to a broadband mobile internet connection to update. This would allow users to get a notification in a usable application when the car is moved, if the device is removed, or if the car alarm goes off. This information can provide useful to police in terms of recovery and can alert owners earlier rather than later.

References

[1] https://www.iii.org/fact-statistic/facts-statistics-auto-theft

[2] Yadav, A., Bose, G., Bhange, R., Kapoor, K., Iyengar, N., & Caytiles, R. D. (2016). Security, vulnerability and protection of vehicular on-board diagnostics. International Journal of Security and Its Applications, 10(4), 405-422.