E2-Chat: A Web-Based End-to-End Encrypted Messaging Service
(CS Technical Paper)

Modular Battery Management System (BMS)
(ECE Technical Paper)

The Privacy Paradox and the Internet of Things (IoT): Understanding the role IoT Devices, Governments, and Businesses have on the Privacy Behavior of Individuals
(STS Paper)

A Thesis Prospectus Submitted to the

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

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

Phillip Phan
Fall, 2020

CS Capstone Project Team Members
Saiteja Bevara
Ashwin Pathi
Rithik Yelisetty

ECE Capstone Project Team Members
Dipesh Manandhar
Nripesh Manandhar
Nikilesh Subramaniam
William Zhang

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

Introduction

Many of the popular online services that Americans use such as Facebook and Google are free. Yet, these services, which include social media websites and online search engines, result in an unprecedented amount of revenue and influence for the companies that own these services. For example, Facebook had an advertising revenue of $69.66 billion and Google had an advertising revenue of $134.81 billion in 2019 (Clement, 2020a; Clement 2020b). However, there is an insidious secret that these companies are hiding from users: the users themselves are the product being sold as their personal data is collected to form an in-depth personal profile. This personal data is then sold to the advertising company with the highest bid in an online auction (Metz, 2015).

While selling one's online data to advertising companies seems relatively innocuous, this private data can be used in more nefarious scenarios by malicious actors. For example, the messages and social media posts of individuals in China are monitored, and individuals are punished if they speak out against the Chinese government (Mitchell & Diamond, 2018). This environment results in a society where individuals are afraid of dissenting against the Chinese government and every facet of an individual's life is subject to monitoring. This example highlights the importance of data privacy as it checks the power of corporations and governments. Therefore, it is critical to have technological advancements and government regulations that preserve the privacy of individuals.

The proposed computer science (CS) capstone project involves creating a web-based end-to-end encrypted (E2EE) messaging service known as E2-Chat, which would preserve the privacy of the individuals that use this messaging service by preventing their messages from being accessible to a third party. Technological advances like E2-Chat are critical to protecting

the privacy of individuals. However, it is up to consumers to use services that protect their privacy. A Pew Research Center report in 2015 shows how 93% of American adults believe that it is important to be able to control who can obtain information about them (Madden & Rainie, 2015). There is, however, a disconnect between how American adults believe that their data privacy is important and their actions since only 9% of respondents reported making changes to their internet or cell phone usage to avoid having their online activities tracked (Madden & Rainie, 2015). This disconnect in the actions of individuals and their personal privacy is colloquially known as the privacy paradox (Williams et al., 2015).

Cisco projects that the number of internet-connected devices per capita will have risen from an average of 8.2 devices in 2018 to 13.6 in 2023, which represents a projected increase of 66% ("Cisco Annual Internet Report (2018–2023) White Paper," 2018). This projected increase in internet-connected devices means that consumers would be overwhelmed by the different possible methods that internet-connected devices can be used to collect their data, exacerbating the privacy paradox. With the widespread prevalence of IoT devices in the last five years, the science, technology, and society (STS) research topic will focus on analyzing the underlying reasons behind why the privacy paradox is pervasive among U.S. adults and recommend methods to mitigate the effects of the privacy paradox.

Unlike the CS capstone project, the electrical and computer engineering (ECE) and STS research projects are not related. The ECE capstone project involves creating a modular battery management system (BMS) prototype to monitor the charge and regulate the temperature of a battery pack in systems such as electric vehicles. The modular design would allow for the BMS to scale up based on the size of a battery pack, and result in easier replacement of components compared to a non-modular BMS.

E2-Chat: A Web-Based End-to-End Encrypted Messaging Service

For a traditional chat service, such as email and short messaging service (SMS), messages are sent through an intermediary service and are stored in a third-party database (Libby, 2019). The sender and receiver of a message then retrieve these messages to view and respond to them. These messages are only encrypted as they are sent to another individual, which means the messaging service provider has access to one's messages. Other third parties can also view an individual's messages if, for example, a malicious actor illegally obtains access to the database containing one's messages or a law enforcement has a subpoena to obtain an individual's message records (Rosen, 2011). Since there is the possibility of third-party actors accessing an individual's messages, users may become fearful of what they say through a messaging service as the contents of the message might be embarrassing to them if it gets leaked online. Taken to an extreme, third-party entities such as authoritarian governments can spy on dissidents and prosecute activists under the guise of combating terrorism or civil unrest. To allow for open discourse free from government censorship and protect people's personal information from hostile third parties, it is critical to have a messaging service where only the sender and receiver of a message can see the messages.

E2EE messaging services are inherently more secure than traditional messaging services as only the sender and recipient see the messages in a chat. The third-party messaging provider is unable to read the messages being sent through an E2EE messaging service. This feat is accomplished by using a private and public key that each user possesses where the public key is visible to any other user and only the individual user has access to their private key (Greenberg, 2014). To send a message, the sender uses the recipient's public key to encrypt the message into a scrambled set of characters. This scrambled message is sent over the internet and when the

receiver obtains the message, this person can decrypt the message back into plaintext using their private key ("WhatsApp Encryption Overview," 2016).

E2EE messaging services rely on mobile devices, since they are portable and do not require the cumbersome transfer of keys around devices. However, current desktop-based E2EE messaging services such as WhatsApp, are only an interface to the mobile version of the messaging service, and still require a smartphone to use their chat services (Greenberg, 2020). In areas with low smartphone usage, such as emerging economies like India, Nigeria, and Indonesia, approximately 45% of the population own smartphones, but more than 60% of them have access to the internet (Silver, 2019). E2-Chat aims to implement a new purely web-based E2EE messaging service, which will enable users to have E2EE communication if they do not own a smartphone.

E2-Chat will support one-to-one chats, group chats, and sending various media such as images, all without the use of an auxiliary mobile device. This project will be developed as part of a group of four using technologies such as React.js, GraphQL, Node.js, and web browser key generation libraries. Previous research on encryption protocols for public/private key exchange such as RSA, or Diffie-Hellman will also be used to implement E2-Chat ("WhatsApp Encryption Overview", 2016). If the project is successful, the data in the database will be fully encrypted and contain no identifiable plain text messages. Since private keys are not stored on the server, these encrypted messages cannot be decoded by third parties. The effectiveness of E2-Chat will be confirmed by verifying that the contents of the database can only be decrypted by the sender and receiver of a message.

Modular Battery Management System (BMS)

Electric vehicles (EVs) have recently gained popularity as an environmentally friendly alternative to vehicles that need gas due to lowering costs and rising consumer awareness about the need to reduce greenhouse gas emissions (Xu & Cao, 2015). The battery is an essential component of the electric vehicle and the battery's performance determines the driving range of EVs. A battery management system (BMS) is needed to prevent the battery from overcharging or receiving high currents which can deteriorate the lifetime of the battery. In addition, a BMS can report important battery information such as the amount of charge stored within a battery, also known as state of charge, and extend the battery lifetime via cell balancing (Brandl et al., 2012). Cell balancing involves redirecting charge to prevent overcharging and over discharging of a battery.

A popular BMS that is commonly used in industry is the Orion BMS ("Orion Li-ion battery management system," n.d.). Along with BMSs, Orion offers a user interface that lets users tweak all the parameters of the BMS. Users can monitor temperature, set current limits and device parameters, see live data being gathered, and configure CAN communications. One downfall of the Orion BMS is that it is not modular. Orion offers different BMS sizes of up to 168 cells. But if a user wants to resize their battery pack, they have to buy a new BMS instead of buying an addon module to their existing BMS. Other BMSs have the same flaw in that they can only be used for a battery pack with a maximum number of battery cells (Plett, 2012).

The modular BMS is a battery management system designed to be usable in a wide range of applications, from electric skateboards, scooters, and bicycles to electric vehicles. The modular BMS will be designed to handle many different pack types and sizes while still providing essential BMS services. The BMS features a modular architecture, with many individual module nodes connected to one main node in a star network. Each module node sends

all measured and calculated data from the battery module it monitors to the main node. The module nodes will also control the passive cell balancing of the module they monitor, based on instructions received from the main node. The main node reads the data from the cell nodes and uses measurements from the battery pack to make decisions about how to protect and balance electric charge throughout the entire battery pack. The main node also communicates to an external device to process or visualize the data, and allows the control settings to be programmed by this external device.

The modular BMS will be designed to handle standard BMS capabilities while also having a modular design that conforms with various technical standards. Afterwards, electrical components will be ordered, and a printed circuit board (PCB) for the main and cell nodes will be designed and manufactured. In addition to the hardware components, the following software will be used to implement the modular BMS: KiCad, GitHub, CADLAB, Mbed OS with PlatformIO, and Onshape CAD.

The Privacy Paradox and the Internet of Things (IoT)

"Hi Alexa" and "Ok Google" are both phrases that consumers have been hearing recently throughout their homes. Consumers have been introduced to internet-connected devices such as smart light bulbs and smart TVs over the past five years. These internet-connected devices, also known as smart devices, have a wider range of capabilities compared to their traditional counterparts as they are able to respond to spoken questions, for example. The increased usage of smart devices in American households has given rise to the moniker, the Internet of Things (IoT), as a descriptor for internet-connected devices that are not normally considered computers and can communicate with each other (Burgess, 2018; Rose et al., 2015). Companies can sell the information obtained from IoT device users to advertisers, which has

opened up a new front in data collection methods as user data has been traditionally collected while a user interacted with a website (Burgess, 2017). Over the course of the next decade, the features in IoT devices will become more robust and powerful, enabling companies and governments to use new methods to tremendously expand the amount of data that is collected from individuals.

At the time of the Pew Research Center report that surveyed American adults' attitudes towards privacy in 2015, IoT devices were generally seen as novelties since first generation IoT devices had limited functionality and were rife with software bugs (Baldwin, 2015). Five years later, however, consumers have grown accustomed to IoT devices due to their convenience and widespread usage in popular media, which would only deepen the effects of the privacy paradox from previously being restricted to one's internet browsing habits. This environment would result in a society where individuals are inundated by smart devices that collect data about every facet of their lives if consumers do not take action to rein in data collection methods.

Actor Network Theory (ANT) is a STS theory that maps shifting networks of relationships in the social and natural worlds (Cressman, 2009). ANT will be used to help answer the STS research question of how the influence of various actors affected the privacy attitudes of the average consumer, and how that has resulted in the widespread prevalence of the privacy paradox among consumers. There are some drawbacks to using ANT as different scholars use ANT and obtain different results for the same research question, which can seem contradictory. These different results occur because there may not be a consensus on how a network should be structured as individuals see the same problems through different lenses. Additionally, ANT primarily consists of empirical, observational evidence, which means that intangibles like values and norms are omitted when discussing why certain networks succeed or fail (Radder, 1990).

One final criticism of ANT is that ANT limits human motivations to pre-established categories or models (Cressman, 2009). Despite these criticisms, ANT is the framework best suited to analyze this research question as ANT provides an extensive structure to explain how various actors contribute to the privacy paradox being prevalent among consumers. ANT will be used to answer the research question with four primary actors in the network: companies, government, IoT devices, and consumers. The relationships between these actors will be analyzed with an emphasis on the consumer's relationship with the other three actors. This analysis will be used to answer why the privacy paradox is prevalent among consumers, and how each actor can implement changes to address the root causes of the privacy paradox.

Methodologies

A literature review will be primarily used to help understand the motivations behind each actor, and the relationships between them. Additionally, this literature review will be used to recommend potential solutions that each actor can take to reduce the effect of the privacy paradox and increase data privacy. The papers for the literature review will be gathered by looking for peer-reviewed papers that propose various explanations behind the privacy paradox. These theories will be backed up by empirical studies on consumer's privacy behavior through surveys and experiments. Keywords that will be used to collect this research include the following: data privacy, privacy paradox, IoT, and social media. The methodology for answering the research question will be organized by first focusing on the relationships between government, companies, and IoT devices. This analysis will be used to contextualize each actor's relationship with consumers, and help evaluate the consumer's relationship with these three actors. This exploration of the network will be used to explain the prevalence of the privacy

paradox among consumers and propose possible actions to combat the privacy paradox.

Conclusion

The CS capstone project will have a functional prototype of E2-Chat completed where users are able to send E2EE messages to each other without needing a smartphone. The effectiveness of the end-to-end encryption implementation will be verified by ensuring that a third-party actor cannot access an individual's message logs without the individual's private key. A technical report detailing how E2-Chat was implemented will also be produced.

For the ECE capstone project, a functional prototype of the modular BMS will be completed. The BMS should be able to monitor the voltage, temperature, and current of the battery pack, and these readings should be visible in the software interface of the modular BMS. Additionally, the BMS should be able to regulate the temperature of the battery pack using fans, and control the battery discharge and charge cycle to preserve the health of the battery pack. A technical report about the modular BMS will also be a deliverable for the ECE capstone.

At the conclusion of the STS research project, a research paper will be produced, which analyzes how the influence of various actors (IoT devices, businesses, governments) affected the privacy attitudes of the average consumer, and how that has resulted in the widespread prevalence of the privacy paradox among consumers. Additionally, possible methods to address the root causes of the privacy paradox that each actor can undertake will be included in the final research paper. Through this analysis, readers will obtain a greater understanding of the trajectory of data privacy over the course of the next decade, and consumer data can be better protected in an increasingly data-driven world.

References

Baldwin, R. (2015, December 23). *2015: The year the Internet of Things jumped the shark* [Engadget]. https://www.engadget.com/2015-12-23-2015-the-year-iot-jumped-the-shark.html

Brandl, M., Gall, H., Wenger, M., Lorentz, V., Giegerich, M., Baronti, F., Fantechi, G., Fanucci, L., Roncella, R., Saletti, R., Saponara, S., Thaler, A., Cifrain, M., & Prochazka, W. (2012). *Batteries and battery management systems for electric vehicles*. 971–976. https://doi.org/10.1109/DATE.2012.6176637

Burgess, M. (2017, July 25). The Internet of Things is a data farm, Roomba won't be its only profiteer. *Wired UK*. https://www.wired.co.uk/article/roomba-data-sell-internet-of-things

Burgess, M. (2018, February 16). What is the internet of things? Wired explains. *Wired UK*. https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot

Cisco Annual Internet Report (2018–2023) White Paper. (2018). Cisco. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Clement, J. (2020, February 28). *Facebook: Advertising revenue worldwide 2009-2019* . Statista. https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/

Clement, J. (2020, February 5). *Google: Annual advertising revenue 2001-2019* . Statista. https://www.statista.com/statistics/266249/advertising-revenue-of-google/

Cressman, D. (2009, April). *A Brief Overview of Actor-Network Theory: Punctualization, Heterogeneous Engineering & Translation*. ACT Lab/Centre for Policy Research on Science & Technology (CPROST).

Greenberg, A. (2014, November 25). Hacker lexicon: What is end-to-end encryption? *Wired*. https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/

Greenberg, A. (2020, January 10). Facebook says encrypting messenger by default will take years. Wired. https://www.wired.com/story/facebook-messenger-end-to-end-encryption-default/

Introduction to battery-management systems. (n.d.). Coursera. Retrieved October 31, 2020, from https://www.coursera.org/learn/battery-management-systems

Libby, K. (2019, November 14). *How SMS works—And why you shouldn't use it anymore*. Popular Mechanics. https://www.popularmechanics.com/technology/security/a29789903/what-is-sms/

Madden, M., & Rainie, L. (2015, May 20). Americans' attitudes about privacy, security and surveillance. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Metz, C. (2015, September 21). Facebook Doesn't Make as much Money as It Could—On Purpose. *Wired*. https://www.wired.com/2015/09/facebook-doesnt-make-much-money-couldon-purpose/

Mitchell, A., & Diamond, L. (2018, February 2). *China's Surveillance State Should Scare Everyone*. The Atlantic. https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/

Orion Li-ion battery management system. (n.d.). Retrieved October 31, 2020, from http://www.orionbms.com/

Plett, G. (n.d.). *Introduction to battery-management systems*. Coursera. Retrieved October 31, 2020, from https://www.coursera.org/learn/battery-management-systems

Radder, H. (1992). Normative reflexions on constructivist approaches to science and technology. *Social Studies of Science*, *22*(1), 141–173.

Rose, K., Eldridge, S., & Chapin, L. (2015). *The Internet of Things: An Overview*. Internet Society. https://www.internetsociety.org/resources/doc/2015/iot-overview/

Rosen, R. J. (2011, July 8). *How your private emails can be used against you in court*. The Atlantic. https://www.theatlantic.com/technology/archive/2011/07/how-your-private-emails-can-be-used-against-you-in-court/241505/

Silver, L. (2019, February 5). *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally*. Pew Research Center. https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/

Singer, N. (2018, April 11). What you don't know about how Facebook uses your data. *The New York Times*. https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html

WhatsApp Encryption Overview. (2016). WhatsApp. https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

Williams, M., Nurse, J. R. C., & Creese, S. (2016). The perfect storm: The privacy paradox and the internet-of-things. *2016 11th International Conference on Availability, Reliability and Security (ARES)*, 644–652. https://doi.org/10.1109/ARES.2016.25

Xu, J., & Cao, B. (2015). Battery management system for electric drive vehicles – modeling, state estimation and balancing. *New Applications of Electric Drives*. https://doi.org/10.5772/61609