Undergraduate Thesis Prospectus

Improving Service in Restaurants with a Smart Coaster

(technical research project in Electrical and Computer Engineering)

The Toxic Battle Between Governments and Technologists over End to End Encryption

(STS research project)

by

Will Define

October 31, 2019

technical project collaborators:
Daniel Ayoub
Taylor Kramer
James Garcia-Otero
Adam El Sheikh

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.

signed: Will _______________ date: 12/6/19

approved: Peter _______________ date: Dec 9, 2019
Peter Norton, Department of Engineering and Society

approved: _______________ date: 12/9/2019
Harry Powell, Department of Electrical and Computer Engineering

General Research Problem

How should engineers incorporate encryption into products?

Encryption is critical to securing technology products. End-to-end encryption is the safest way to secure data as it reduces the number of parties who may break the encryption (EFF Surveillance Self-Defense Guide). Unfortunately, there are indirect consequences from E2EE; certain crime detection and investigative efforts would be impeded. When implementing encryption, engineers must balance tradeoffs, security, privacy and public safety, as well as stakeholders, users and the general public.

Improving Service in Restaurants with a Smart Coaster

Can restaurants improve service with a smart coaster that automatically alerts staff of an empty cup?

This capstone project will be completed in the Electrical and Computer Engineering department by Daniel Ayoub, Taylor Kramer, James Garcia-Otero, Adam El Sheikh, and Will Define under advisement of Professor Harry Powell. This project seeks to create a novel internet enabled device that can be deployed at scale in restaurants to alert waitstaff of an empty drink and thereby improve service. The project will discover whether this IoT approach is beneficial to restaurants and furthermore discover how to implement such a system so that it is easy to use.

The coaster will consist of a custom designed PCB housed within a watertight 3D printed case. The case will contain pressure sensors and a microcontroller to read them. The microcontroller will communicate these readings over a separate encrypted WIFI network. The network will include a desktop computer running software to interface with waitstaff. The smart coaster will include its own power station that will charge the coaster inductively so that the design may be entirely watertight. Functionally, the coaster will be assigned a drink by the server when placed on a table. Then the coaster will alert the server whenever the drink is empty. The prototype may only include one coaster, but the system will be scalable to support many coasters.

Prior art includes a smart coaster produced by students at Saarland University in Germany in 2005 (Butz 2005). This project identified empty cups with force sensors, but did not include inductive charging.

The Toxic Battle Between Governments and Technologists over End-to-end Encryption

How do cybersecurity researchers and privacy advocates compete with world law enforcement agencies to influence end-to-end encryption?

End-to-end Encryption

End-to-end encryption (E2EE) is a form of encryption used in messaging apps. In a typical system without E2EE, a message is encrypted in transit and decrypted to plaintext at some point on the server. In an E2EE system, the message is encrypted by the sender such that it can be decrypted only by the receiver. The server can never know the contents of the message. E2EE enhances privacy by preventing the messaging service from sharing message content with law enforcement or hackers.

End-to-end Encryption Controversy

E2EE is controversial. Privacy advocates see E2EE as the gold standard for protecting communication from governments and hackers. Law enforcement sees E2EE as a barrier to fighting crime. This debate is the latest in a long line of encryption battles between law enforcement agencies and privacy advocates.

End-to-end Encryption Usage

As of 2019, some messaging apps use E2EE, including IMessage and WhatsApp. Facebook messenger does not use E2EE but plans on deploying it soon (Zuckerberg 2019). The two largest messaging apps in China, WeChat and QQ, do not use E2EE. Skype claimed to use E2EE, but the Snowden leaks revealed an NSA backdoor (Greenwald 2013).

Cybersecurity Researchers

Cybersecurity researchers are closely related and overlap significantly with privacy advocates. Here they are distinguished so that the technical and ethical perspectives on E2EE can be evaluated separately. Cybersecurity researchers promote E2EE to enhance security. Opponents of encryption often advocate for special back doors. Cybersecurity researchers have established principled opposition to back doors. They argue that if back doors are built into encrypted systems, hackers will find these doors (Stepanovich et al. 2018). Additionally, even an ideal backdoor would add complexity risking exploitable errors; proverbially "complexity is the enemy of security" (Abelson et al. 2015). These arguments have been validated over the past 30 years. 15 top researchers, in a paper advocating against back doors, discussed their opposition to the inclusion of the NSA's Clipper Chip in consumer electronics in the 1990's. With the Clipper Chip, the NSA could have decrypted any voice data. Clipper was never widely adopted, and contained bugs that could encrypt messages without creating a backdoor (Blaze 1994). 20 years later, the researchers used the same arguments against backdoors to E2EE as against the Clipper Chip (Abelson et al. 2015).

Privacy Advocates

Privacy advocates advocate by widely publishing pro encryption material and narrowly influencing the technologists implementing encryption. In response to the Snowden leaks of

2013, the Electronic Frontier Foundation published the free eBook, *The End of Trust*. The book highlighted the dangers of governmental spying in private communication (Eggers at al. 2018). Privacy advocates make a global argument. If tech companies grant backdoors to US or Australian government agencies, authoritarian regimes would ask the same. The same backdoors used to catch pedophiles could be used to persecute dissidents (Roth 2017). Many messaging platforms are built in authoritarian regimes, notable China, that do not abide by western privacy standards. While the United Nations supports E2EE, privacy advocates worry that laws granting backdoors in liberal democracies will erode international support for E2EE. By presenting themselves as global champions of democratic values, privacy advocates can put government agencies in a difficult position.

Many technologists value privacy and therefore favor encryption. Witness the comments on Hacker News, a technologist watering hole, in response to encryption news (Hacker News, Apr 2016; July 2016). The EFF accelerates this sentiment. After Google introduced E2EE in Allo in opt-in mode, the EFF retweeted employee Nate Cardozo: “Hey @google, what the shit? You support encryption? Turn it on by default, or don't bother playing,” (Williams 2016). With opt-in encryption, privacy conscious users can protect their messages while most remain unencrypted on server. The EFF provides a platform for the E2EE supportive technologists to buttress technologist support for E2EE.

Law Enforcement Agencies

The loudest opponents to E2EE have been law enforcement agencies. Australia requires messaging platforms to grant access to encrypted messages on request (Parliament of Australia 2018). Cybersecurity officials in the UK propose a “Ghost protocol” with which a government official can be added as a participant in an encrypted communication (Levy et al. 2018). US and

UK officials signed a letter asking Facebook to not go through with plans encrypt to Facebook Messenger (Patel et al. 2019). There are dissenting voices in government. General Hayden, former director of the NSA and CIA, has argued in favor of E2EE (Ashbrook 2016). Nevertheless, opposition to E2EE is pervasive in law enforcement agencies.

These agencies warn that E2EE shields terrorism, child exploitation, and crime rings. The letter to Facebook points out that more than 90% of the 18.4 million reports to the US National Center for Missing and Exploited Children come from Facebook. The UK estimates that with such data, law enforcement protects 3000 children every year (Patel et al. 2019). Many of these reports come from Facebook's automated monitoring of messages on Messenger for illegal content. Since the messages are flagged by Facebook internally, law enforcement could not investigate such crimes through warrants. Indeed, the letter asks Facebook to continue automatic content monitoring (Patel et al. 2019). This letter contains no technical details, so security implications cannot be directly discussed. The Ghost Protocol is a rare example of a law enforcement agency providing technical details for a E2EE backdoor. With the Ghost Protocol, a messaging service could add a law enforcement agent as an invisible member of a group chat effectively sidestepping E2EE (Levy et al. 2018). It would force companies to lie about who is receiving texts. 47 organizations, including major tech companies, have rejected the proposal citing user trust above all (Access Now et al. 2019).

Tech Companies

Because tech companies implement E2EE, they have tremendous power in their tug of war with cybersecurity researchers, privacy advocates, and law enforcement. Recently, Tech companies have moved towards E2EE. A subsection of their users strongly value privacy and security while few users are passionately opposed to E2EE. Witness the consensus in favor of

E2EE in a NY Times comments section (Perlroth 2019). Tech companies, therefore, have an economic incentive to promote E2EE and its values. The anti-Ghost Protocol letter cites values such as “fundamental human rights including privacy and free expression” (Access Now et al. 2019). Meanwhile, there are few economic incentives to not implement E2EE. Australia’s Assistance and Access Act, the strongest regulation against E2EE, faced significant backlash and subsequently watered down (Digital Rights Watch 2019). Facebook received some positive publicity by promoting their efforts to detect child exploitation (Davis 2018). However, Facebook faces separate privacy concerns related to sharing personal data with third parties. Therefore, the company has more to gain by repairing its image around privacy.

References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., … Weitzner, D. J. (2015, July 6). Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications. http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

Access Now, Big Brother Watch, Blueprint for Free Speech, Center for Democracy & Technology, Defending Rights and Dissent, Electronic Frontier Foundation, … Zimmerman, P. (2019, May 22). https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Letter_to_GCHQ_on_Ghost_Proposal_-_May_22_2019.pdf

Ashbrook, T. (2016, March 1). Michael Hayden: America Is Safer With End-To-End Encryption https://www.wbur.org/onpoint/2016/03/01/michael-hayden-nsa-encryption

Blaze, M. (1994). Protocol Failure in the Escrowed Encryption Standard. *AT&T Bell Laboratories*. https://www.mattblaze.org/papers/eesproto.pdf

Butz, A., & Schmitz, M. (2005). Design and applications of a beer mat for pub interaction. *Extended Proceedings of the Seventh International Conference on Ubiquitous Computing*. http://www.mmi.ifi.lmu.de/pubdb/publications/pub/butz2005ubicomp/butz2005ubicomp.pdf

Davis, A. (2019, November 14). New Technology to Fight Child Exploitation. https://about.fb.com/news/2018/10/fighting-child-exploitation/.

Digital Rights Watch. (2019, December 4). Major amendments to encryption laws are a step in the right direction. https://digitalrightswatch.org.au/2019/12/04/major-amendments-to-encryption-laws-are-a-step-in-the-right-direction/.

EFF Surveillance Self-Defense Guide. "End-to-End Encryption". Electronic Frontier Foundation. https://ssd.eff.org/en/glossary/end-end-encryption.

Eggers, D. J., Thompson, S. J., Wachter-Boettcher, S. J., Angwin, J. J., Paglen, T. J., & Snowden, E. J. (2018). *The End of Trust*. https://www.eff.org/document/end-trust-0

Greenwald, G. (2013, June 7). NSA Prism program taps in to user data of Apple, Google and others. The Guardian. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Hacker News. UK surveillance bill includes powers to limit end-to-end encryption: (2016, July 5).https://news.ycombinator.com/item?id=12159942.

Hacker News. WhatsApp Rolls Out End-To-End Encryption to Its Over 1B Users: (2016, April 8).https://news.ycombinator.com/item?id=11453812.

Levy, I., & Robinson, C. (2018, November 29). Principles for a More Informed Exceptional Access Debate. https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate.

Parliament of Australia. The Assistance and Access Act 2018. (2018, December 6). https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption.

Patel, R. H. P. P., Barr, W. K., McAleenan, K., & Dutton, H. P. Open Letter: Facebook’s “Privacy First” Proposals. (2019, October 4). https://www.justice.gov/opa/press-release/file/1207081/download

Perlroth, N. (2019, November 19). What Is End-to-End Encryption? Another Bull's-Eye on Big Tech. https://www.nytimes.com/2019/11/19/technology/end-to-end-encryption.html.

Roth, K. (2017, June 28). The battle over encryption and what it means for our privacy. https://www.hrw.org/news/2017/06/28/battle-over-encryption-and-what-it-means-our-privacy#.

Stepanovich, A., & Karanicolas, M. (2018, March 2). Why An Encryption Backdoor for Just the "Good Guys" Won't Work. https://www.justsecurity.org/53316/criminalize-security-criminals-secure/.

Williams, K. B. (2016, May 31). Facebook Messenger to feature optional end-to-end encryption: report. https://www.eff.org/mention/facebook-messenger-feature-optional-end-end-encryption-report.

Zuckerberg, M. (2019, March 6). A Privacy-Focused Vision for Social Networking. https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/.