Undergraduate Thesis Prospectus

Designing Secure and Usable Wake-Up Words

(technical research project in Computer Science)

Reclaiming the Road: How Agendas for Car-free Cities are Advancing in the COVID Era

(sociotechnical research project)

by

Timothy Han

November 2, 2020

technical project collaborators:

Joshua Sahaya Arul
Andrew Wang

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.
Timothy Han

Technical advisor: Yuan Tian, Department of Computer Science

STS advisor: Peter Norton, Department of Engineering and Society

Timothy Han
STS 4500 (3:30)
December 11, 2020

General Research Problem

How can current sociotechnical systems be modified to be more intuitive and people-centered?

Though innovation is ubiquitous, not all of it serves human wellbeing or social benefit. Technology consumerism favors innovation for innovation's sake, and the effects can be hazardous. These dangers are evident when we look at injuries and accidents in the workplace. Experts typically attribute over 90 percent of road and workplace injuries to human error. Yet because so-called "human error" occurs in complex settings in which automated systems, interface design, and device usability are deeply implicated, such conclusions are dubious. Investigators who blame human users should more carefully consider why the system they used failed them (Norman, 2018). It will be useful to examine technology as an enabler of a successful solution and not as the default tool, include end-users as integral participants of the design process, and remain cognizant of ethics and sustainability to bake in these values from the start (Niemala et al., 2020).

Designing Secure and Usable Wake-Up Words

How can we design wake-up words for smart speakers which are both secure and usable, reducing the rate of accidental triggers and malicious use?

My technical advisor is Professor Yuan Tian in the Computer Science department. I will be working with Joshua Sahaya Arul and Andrew Wang, both of whom are computer science majors in the Engineering School. The technical project is about designing secure and usable wake-up words for voice-controlled devices. There are millions of voice activated assistants in multitudes of devices all across the world, from phones (Siri, Google Assistant) to home speakers such as Amazon Alexa and Google Homes. These voice-controlled devices are always listening to audio input, searching for a keyword known as the "wake-word" before streaming

subsequent audio input to the cloud for further processing. Unfortunately, when wake-words were first designed, very few were designed with security or usability in mind – Siri was the name of an employee in Norway. Because of this, accidental triggers can occur from anything, ranging from normal conversation, to TV and radio, to other malicious voice-controlled device skills. For example, the words “cocaine noodles” or “OK cool” can trigger a Google Home, who’s wake-up word is “OK Google” (Schonherr et al., 2020). An accidental trigger is a case of privacy failure, meaning the device will stream audio without user consent to be processed in the cloud, possibly leaving an avenue for exploitation and stealing of critical information.

The goal of this project will be to design wake-up words which limit the number of accidental triggers from misconstrued audio signals. A constraint of the project is working from home due to COVID-19, limiting the testing capabilities of any solution we create as we cannot test with multiple live voices.

Work on voice-controlled input confusion began in 2015 with Vaidya et al., which showed that the words “Cocaine Noodles” could be used to wake a Google Home and perform sensitive tasks such as sending texts or calling a number. Later studies expose an attack called “skill squatting”, the practice of naming skills to very similar names to others in order to take advantage of imperfect transcription and retrieve sensitive user data. For example, a skill could be called “Capital Won” instead of the banking skill “Capital One”, and trick users to give up bank information (Zhang et al., 2019). State of the art work in Schonherr et al. has been done on automating the process of finding unsafe wake-up words, and through this technical project, we hope to use machine learning algorithms, along with the knowledge obtained from the state of the art work and the data set published from said work of 1,000 accidental triggers to create a

model of usable and secure wake-up words. Hopefully, this research will be useful in changing the design of wake-up words to be more intentional and secure.

Reclaiming the Road: How Agendas for Car-free Cities are Advancing in the COVID Era

How have advocates of car free cities advanced their agendas in the COVID-era transportation freeze?

The 2020 pandemic has disrupted urban transport worldwide. Stay-at-home orders and avoidance of buses and other transit modes have given car-free advocacy groups a unique opportunity to show the residents of cities what a car-free future might look like – and decide for themselves which version of the city they prefer. The pandemic may be an opportunity to change "habits, behavior, and thinking paradigms, and to accept new, automated, healthier, and improved means of urban mobility" (Ceder, 2020).

Researchers have already begun investigating the effects of the pandemic on urban transport. In Portland, Oregon, traffic fell up to 50 percent from December 2019 to March 2020. In Salt Lake City, volume reduced by up to 75 percent of normal traffic levels (Tierney, 2020). Fatal collisions have fallen by half in California, saving the public $40 million a day (Shilling, 2020). Fleisher et al. (2020) urges immediate investment in public transit, so that it will be available as conditions improve. France will require Air France to eliminate all short-haul flights wherever rail is available; in the UK, a new "Jet Zero" council seeks a "greener restart" after the pandemic passes (Naimoli, 2020). Such initiatives may find equivalents in urban transport.

Advocates of car-free cities include urbanists. In its general sense, urbanism is the study of how people interact with an urban environment, but the word also more specifically characterizes a movement called, in full, new urbanism. To new urbanists, urbanism is a value:

that "well-designed cities, towns, neighborhoods, and public places help create community: healthy places for people and businesses to thrive and prosper" (CNU, 2020). To urbanists, car domination and car dependency are incompatible with functioning, healthy, inclusive, and sustainable cities. Instead, urbanists favor of mass transit and active mobility (Naimoli, 2020). To pursue this agenda, they typically favor policy innovation over technology innovation.

Participants include car-free advocacies such as Auto-Free New York, which seeks "devehicularization" (Haikalis, 2020). The New Urban Mobility Alliance (NUMO) espouses the Shared Mobility Principles, which were codified in 2017. The principles prioritize people over vehicles in urban planning. NUMO and other organizations maintain a crowdsourced database of mobility responses to the 2020 pandemic (NUMO, 2020). The League of American Cyclists advocates for bike lanes, public transit, and more pedestrian space to make urban cycling more accessible and safer (Whitaker, 2020). The San Francisco Bay Area Planning and Urban Research Association (SPUR) promotes people-friendly planning in San Francisco, including mass and active transit, through research and policy proposals (Fleisher et al., 2020). Social entrepreneurs such as Sindile Mavundla of Khaltsha Cycles seek to "increase ridership through social events" and promote safe biking infrastructure. During the pandemic the company has provided bicycles to essential workers; its staff hopes to promote new cycling habits that endure long after the pandemic (Mavundla et al., 2020).

References

Ceder, A. (2020). Urban mobility and public transport: future perspectives and review. *International Journal of Urban Sciences,* doi: 10.1080/12265934.2020.1799846.

CNU. (n.d.). Congress for the New Urbanism. The Movement. https://www.cnu.org/who-we-are/movement

Fleisher, A., Cohen, S., Amin, R., Deutsch-Gross, Z., & Kiner, L. (2020). The Future of Transportation: Harnessing private mobility services to support the public good (Arieff A., Ed.). SPUR (San Francisco Bay Area Planning and Urban Research Association). doi:10.2307/resrep26075.3.

Haikalis, G. (2020, September 1). Welcome to Pandemic New York!. AUTO-FREE-NEW YORK!. http://www.auto-free.org/index.html

Mavundla, S., Yasin, A., Zayas, G., Norman, P., & Pardo, C. (2020, September 21). Speakers Corner Part 2: Taking back the streets [Webinar]. World Car Free Day. https://www.bigmarker.com/car-free-day-cic/World-Car-Free-Day-Summit-Speakers-Corner-Part-2-Taking-back-the-streets?bmid=12f5a51f06c0

Naimoli, S., & Tsafos, N. (2020). (Rep.). Center for Strategic and International Studies (CSIS). doi:10.2307/resrep25199

Niemelä, M., Ikonen, V., Leikas, J., Kantola, K., Kulju, M., Tammela, A., Ylikauppila, M.. (2014, Jul.). Human Driven Design: A Human-Driven Approach to the Design of Technology. 11th IFIP International Conference on Human Choice and Computers (HCC). pp.78-91.

Norman, D. (2018). People-Centered (Not Tech-Driven) Design. *Encyclopædia Britannica.*

NUMO (2020). New Urban Mobility Alliance. COVID Mobility Works. https://www.numo.global/spotlight-on/responding-covid-19/covid-mobility-works

Schonherr, L., Golla, M., Eisenhofer, T., Wiele, J., Kolossa, D., & Holz, T. (2020). Unacceptable, where is my privacy? Exploring Accidental Triggers of Smart Speakers. arXiv preprint arXiv:2008.00508.

Shilling, F., Dr., & Waetjen, D., Dr. (2020). Special Report(Update): Impact of COVID19 Mitigation on Numbers and Costs of California Traffic Crashes. California: Road Ecology Center at UC Davis. https://roadecology.ucdavis.edu/files/content/projects/COVID_CHIPs_Impacts_updated_415.pdf

Tierney, L. F. (2020). COVID-19 Traffic Volume Trends. https://www.ite.org/about-ite/covid-19-resources/covid-19-traffic-volume-trends/

Vaidya, T., Zhang Y., Sherr M., & Shields C. (2015). Cocaine Noodles: Exploiting the Gap between Human and Machine Speech Recognition. USENIX Workshop on Offensive Technologies, ser. WOOT ’15.

Whitaker, C. (2020, April 14). Lobbying in a time of covid-19. https://bikeleague.org/content/lobbying-time-covid-19

Zhang N., Mi X., Feng X., Wang X., Tian Y. and Qian F. (2019). Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems. *2019 IEEE Symposium on Security and Privacy (SP).* 1381-1396. doi: 10.1109/SP.2019.00016.