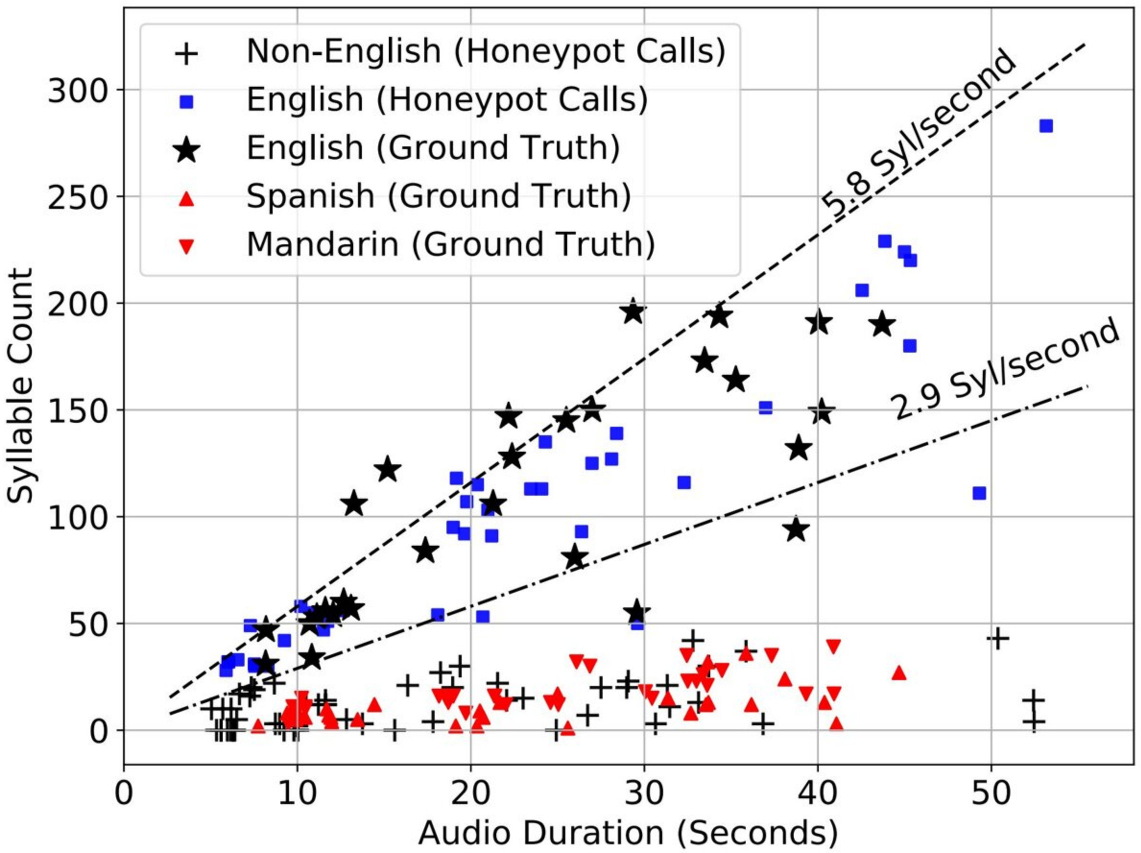
TechXplore

A new weapon in the war on robocalls

August 8 2023, by Matt Shipman



Classifying English and Non-English calls. Credit: *Diving into Robocall Content with SnorCall* (2023)

The latest weapon in the war on robocalls is an automated system capable of analyzing the content of these unsolicited bulk calls to shed light on both the scope of the problem and the type of scams being perpetuated by robocalls. The tool, called SnorCall, is designed to help regulators, phone carriers and other stakeholders better understand and monitor robocall trends—and take action against related criminal activity.

"Although telephone service providers, regulators and researchers have access to call metadata—such as the number being called and the length of the call—they do not have tools to investigate what is being said on robocalls at the vast scale required," says Brad Reaves, corresponding author of a paper on the work and an assistant professor of computer science at North Carolina State University.

"For one thing, providers don't want to listen in on calls—it raises significant privacy concerns. But robocalls are a huge problem, and are often used to conduct criminal fraud. To better understand the scope of this problem, and gain insights into these scams, we need to know what is being said on these robocalls."

"We've developed a tool that allows us to the characterize the content of robocalls," Reaves says. "And we've done it without violating privacy concerns; in collaboration with a telecommunications company called Bandwidth, we operate more than 60,000 phone numbers that are used solely by us to monitor unsolicited robocalls. We did not use any phone numbers of actual customers."

The new tool, SnorCall, essentially records all robocalls received on the monitored phone lines. It bundles together robocalls that use the same audio, reducing the number of robocalls whose content needs to be analyzed by around an order of magnitude. These recorded robocalls are then transcribed and analyzed by a machine learning framework called Snorkel that can be used to characterize each call.

"SnorCall essentially uses labels to identify what each robocall is about," Reaves says. "Does it mention a specific company or government program? Does it request specific personal information? If so, what kind? Does it request money? If so, how much? This is all fed into a database that we can use to identify trends or behaviors."

As a proof of concept, the researchers used SnorCall to assess 232,723 robocalls collected over 23 months on the more than 60,000 phone lines dedicated to the study.

"Those 232,723 robocalls were broken down into 26,791 'campaigns,' or unique audio files," Reaves says. "And we were able to extract a tremendous amount of information from those campaigns."

Perhaps most importantly, the researchers were able to extract the phone numbers used in these scams. Robocallers often "spoof" the number they are calling from, making it impossible to tell where the call actually originated. However, scammers increasingly encourage the people receiving robocalls to call a specific phone number. This may be to resolve a (fictional) tech support issue, resolve a (fictional) tax problem, resolve a (fictional) issue with Social Security, and so on.

"Scammers can fake where a robocall is coming from, but they can't fake the number they want their victims to call," Reaves says. "And about 45% of the robocalls we analyzed did include this 'call-back number' strategy. By extracting those call-back numbers, SnorCall gives regulators or law enforcement something to work with. They can determine which phone service providers issued those numbers and then identify who opened those accounts."

The proof of concept analysis also shed light on how specific robocall campaigns operate over time.

"For example, we saw very clear trends in the number of robocalls about Social Security scams being made during the pandemic," Reaves says.

"As COVID shut down offices, we saw the number of Social Security scam robocalls dwindle to nearly zero. And then saw the number of these scam calls ramp back up as COVID restrictions were lifted. This tells us that Social Security scam robocall operations are based in offices—they weren't able to adjust to conditions where the people behind those robocalls would have to work from home. If nothing else, it helps us understand the level of scale and organization behind these robocall Social Security scams."

One of the other advantages of incorporating the Snorkel framework into SnorCall is that Snorkel makes it relatively easy to modify SnorCall to meet stakeholder-specific needs.

"For example, if investigators want to focus on a new scam topic, Snorkel is very good at identifying key terms or phrases associated with topics," Reaves says. "This could be a valuable feature for investigators who are focused on specific types of criminal fraud."

"Our findings demonstrate how illegal robocalls use major societal events like student loan forgiveness to develop new types of scams," says Sathvik Prasad, a Ph.D. student at NC State and first author of the paper. "SnorCall can aid stakeholders to monitor well-known robocall categories and also help them uncover new types of robocalls."

Stakeholders who are interested in this work can learn more about the Reaves lab's overarching efforts at https://robocall.science.

"There's no way we could have done this work without the collaboration of industry partners, including Bandwidth," Reaves says. "And we are definitely interested in working with other companies in the telecom and tech sectors to help us move forward with efforts to address robocalls in a meaningful way."

The paper will be presented Aug. 9 at the USENIX Security Symposium.

More information: Paper: www.usenix.org/system/files/se … repub-344-prasad.pdf

Provided by North Carolina State University

Citation: A new weapon in the war on robocalls (2023, August 8) retrieved 13 May 2024 from https://techxplore.com/news/2023-08-weapon-war-robocalls.html