ACM NEWS

Picking Locks with Audio Technology

By Paul Marks
Commissioned by CACM Staff
August 13, 2020
Comments

VIEW AS: SHARE:

The next time you unlock your front door, it might be worth trying to insert your key as quietly as possible; researchers have discovered that the sound of your key being inserted into the lock gives attackers all they need to make a working copy of your front door key.

It sounds unlikely, but security researchers say they have proven that the series of audible, metallic clicks made as a key penetrates a lock can now be deciphered by signal processing software to reveal the precise shape of the sequence of ridges on the key's shaft. Knowing this (the actual cut of your key), a working copy of it can then be three-dimensionally (3D) printed.

This discovery of a major vulnerability in the physical keys that millions of us use to secure domestic and workplace doors and lockers was made by cyberphysical systems researcher Soundarya Ramesh and her team at the National University of Singapore. At the 21st International Workshop on Mobile Computing Systems and Applications (HotMobile 2020) in

The sound of your key being inserted into the lock gives attackers all they need to make a working copy of your front door key.

Credit: Jacob Black-Lock

Austin, TX, in early March, Ramesh revealed how their technique works.

What's being attacked by the NUS team are the keys to pin-tumbler locks, best known as Yale or Schlage keys, though those are just the market leaders and a whole host of other firms make them, too. Inside such locks, six metal pins, affixed to springs, are pushed up to different heights by the ridged teeth on the key, or kept low by the voids between the ridges. When all six spring-loaded pins are pushed to the correct height by the right key, the tumbler containing them is freed to turn, allowing the lock to be opened. Such a lock typically has something of the order of 330,000 possible key shapes.

Usually, an attack on such a lock requires an expert lock picker with special instruments, or at least some cleverly improvised ones, to nudge the pins to the correct heights and unlock the mechanism. However, such an attack has one major drawback to the attacker: it only gets them into a protected space once. To get in again, they'd have to again pick the lock (or its replacement), with all the risks of discovery that entails.

What attackers really need is a copy of the key so they can come and go as they please, and the NUS team worry that criminals might harness technology to obtain it. How could they go about it, and if they succeed, what countermeasures might be necessary?

The NUS team, which studies sensing and embedded and network security, previously investigated potential future crimes that tech might allow to happen. Last year, for instance, they developed a way of fingerprinting the sound of parcel courier drones, to distinguish them from criminal attack drones that might impersonate the real thing to steal valuable parcels awaiting pickup.

"Our research group leverages information from the physical environment that is seemingly of no utility, to either develop better applications or compromise existing ones. So, we began to wonder if we can utilize the sound produced during key insertion, which has no utility of its own, to compromise physical lock security," says Ramesh.

She says they had strong inspiration for a sensor-based approach from a 2018 safecracking project in which gyroscopic sensors in a smartwatch were used by a Wichita State University-led team to sense the degree of rotation of the wrists of people using a combination lock on a safe. Recalls Ramesh, "By inferring the degree of lock rotation from sensors in the smartwatches worn by users, they were able to crack the combination."

Could sensor data from what Ramesh calls "the ubiquitous good-quality microphones" in the latest smartphones be used to infer the cut of a key from the sound made as the ridges push the lock's pins on key insertion? To find out, the NUS team developed and tested what it calls SpiKey, an end-to-end attack technique for, as its name suggests, spying on Yale/Schlage type keys and using signal processing software to infer their correct shapes.

Acquiring the Audio

Their first task was to work out how to surreptitiously acquire the audio from a key insertion, and the researchers suggest no less than five ways of going about it. First, in a walk-by attack, a spy simply walks behind somebody just as they unlock a door or locker, holding their phone out to furtively record the sound of the key going into the lock. So far, though, they have only done this with the phone an unrealistic 10cm (nearly four inches) from the lock. "We are still working on making this attack realizable," says Ramesh.

Their second method takes another tack entirely: install malware on a victim's smartphone (or smartwatch) so it records and transmits key insertion audio via an Internet or 4G backchannel. Such viruses are already known in the wild.

Third, they believe an attacker might hack a product like a domestic Internet of Things (IoT) device that contains a microphone, like a video doorbell, which is next to the lock, and acquire audio over the air. Again, this is a known attack vector.

The fourth trick might involve long-distance microphones, the NUS team suggest, while a fifth might involve installing hidden microphones in a corridor of a set of target offices; over time, they suggest, attackers could quietly harvest door key audio for multiple offices.

Once they have a key-insertion audio file, SpiKey's inference software gets to work filtering the signal to reveal the strong, metallic clicks as key ridges hit the lock's pins [and you can hear those filtered clicks online here]. These clicks are vital to the inference analysis: the time between them allows the SpiKey software to compute the key's inter-ridge distances and what

locksmiths call the "bitting depth" of those ridges: basically, how deeply they cut into the key shaft, or where they plateau out. If a key is inserted at a nonconstant speed, the analysis can be ruined, but the software can compensate for small speed variations.

The result of all this is that SpiKey software outputs the three most likely key designs that will fit the lock used in the audio file, reducing the potential search space from 330,000 keys to just three. "Given that the profile of the key is publicly available for commonly used [pin-tumbler lock] keys, we can 3D-print the keys for the inferred bitting codes, one of which will unlock the door," says Ramesh.

What can be done about the risk this poses to homes, offices, and even your gym locker? Apart from inserting the key in the lock very quietly and slowly, as alluded to earlier, Ramesh suggests the key ridges that generate the clicks could be "smoothed out so that they are not pointed anymore" to reduce the chance of an acoustic attack.

"My next step will be to explore the feasibility of a generic defense solution against such attacks," she says.

Experts are skeptical key insertion audio will be easy to acquire. "SpiKey seems a novel approach, and the claims of results seem promising, but in a lot of cases acquiring the audio of the 'unlock' could be tricky. So whilst this is a potential threat, in reality it may be a limited one," says Graeme Horsman, a digital and mobile forensics specialist at Teesside University in Middlesbrough, U.K.

Also skeptical was Chris Mitchell, CEO of Audio Analytic in Cambridge, U.K., which uses machine learning to recognize everyday sounds beyond speech and music, in products like smart speakers. When told of the SpiKey work, Mitchell decided to measure the sound pressure levels emitted as a key penetrates a door lock.

"Making this work in the real world requires an in-depth understanding of the sound environment," Mitchell says. "Our quick analysis is that from a distance of 5 to 10 cm, the clicks range from sound pressure levels between 60 to 90 dBA. The loudest click when the key is fully in the lock was 80 to 90 dBA. That is pretty loud, and therefore straightforward for a high-quality microphone to detect."

Mitchell has caveats, however; other sounds, like the jangling of the victim's key ring, or even nearby traffic, could mask the click sequence SpiKey requires. "A single key on its own would not present too much of a problem, but from a real-world point of view, how many people hold

a single key?"

However, Mitchell sees other ways SpiKey could work. "A major challenge is the speed of insertion. To allow for changing [insertion] techniques, you would want to capture a number of recordings over a period of time to increase your chances of success. So you would need to surreptitiously install a high-quality microphone near a person's front door lock, collect data over a period of time, build a model that allowed for different insertion techniques, and then run your model."

Given what it will take to make a success of this attack, Mitchell reckons SpiKey is best aimed at higher-stakes crime, rather than "domestic burglars who don't have a background in acoustic sciences or machine learning."

Mitchell foresees one really great application for SpiKey: in Hollywood. "It sounds like a really good concept for an 'Oceans 14' movie, " he says.

Paul Marks *is a technology journalist, writer, and editor based in London, U.K.*

No entries found