Can't Keep Them Away: The Failures of Anti-Stalking Protocols in Personal Item Tracking Devices (Transcript of Discussion)

Kieron Ivy Turk[1] [0000−0002−4705−4749], Alice Hutchings[1] [0000−0003−3037−2684], and Alastair R. Beresford[1] [0000−0003−0818−6535]

University of Cambridge

Christelle Gloor: It seems like all of those anti-tracking apps or measures that you can take, put the burden on the person who might be stalked to figure this out. It seems very backwards to me. Shouldn't there be a burden of proof for the people who do use those trackers that they're actually using it to track something that is theirs? For example, to track my purse, I set it so that only my phone is going to be able to see this tracker. To prove that I am actually tracking myself, I will tell you I'm going to work here, then I'm going to do this and that and only after this is proven can you do it? Can you activate [the tracker] for a certain amount of time until you have to redo some kind of check like this?

Reply: So, you could. It would make it incredibly hard to use for its legitimate use of finding lost items. If you accidentally leave your keys at home and it says you're not allowed to see where the tracker is until you get within range of it and you're at work and trying to find where you've left something, you're then in a bit of a sticky situation. I agree that it would be good to move the onus away from the vulnerable users who in many cases have no idea they're being tracked at all. But yes, suggestions around that will be useful.

Christelle Gloor: I feel like in some way, because this can do so much damage, the lessened usability for the people who are using those trackers might be a good compromise in a way because it does make so much damage?

Reply: Yes, agreed.

Alex Shafarenko: The tracker announces itself loudly, less loudly, et cetera, but everybody's carrying a mobile phone with them, so why can't you have an app that finds trackers around and all the announcement is done by that app to you, to your smartwatch for instance? So that you're not embarrassed though, you don't have to advertise to everybody that you've discovered that you've been bugged, right?

Reply: That currently exists with AirGuard, although that's only available for Android users[1] and they've only so far done it with AirTags and Tile trackers. But yes, it involves tracking all nearby Bluetooth announcements of the devices

[1] As of April 17th, AirGuard is also available on iOS.

and seeing what's nearby, what's following you. There is a risk of false positives, so you might have your own devices that these apps don't recognise. If they're registered with your own device, then that has to be communicated within the app. Apple sort of gets around this with AirTags by only having the trackers emit lost beacons when it's been separated from the owner for at least an hour. And then it's every 15 minutes. So if you're looking at generic devices that may be following you, you have to look at just generic Bluetooth addresses, that's going to give you more false positives. Perhaps a better example of false positives would be a family member you're travelling with or your partner as their devices are not registered to your phone, but they will still be following you around.

Harry Halpin: One false positive I actually had happened last week as I was on a tour bus with other people that had AirTags on and for the entire time I was on the tour bus, I was notified that was being stalked. And of course, I talked to the other people on the tour bus and they had AirTags enabled and the same bus for a day and they were following me for that day. I was wondering are there any alternatives to the tags that have kind of longer ranges that are being worked on in terms of research?

Reply: There are GPS trackers available and there are some use cases of those being used for stalking. Those are especially commonly used for car theft because it's easier to guarantee they're going to be in range. The problem with those is they're more expensive and they are made for tracking things long distance, so they tend not to have any anti-stalking in, whereas the media attention AirTags have gotten for being used for stalking has led to them implementing anti-stalking. GPS trackers are being used as well, they are just less common because of price.

Ross Anderson: Another solution which I actually put up on my webpage as a possible student project is that you could have a track me not feature. So perhaps our very eager European legislators could require Apple to provide a feature whereby I can put a switch in my iPhone saying neither I nor anybody within 20 metres of my location may be tracked by an AirTag. That's trivial to do, technically. It would require the force of the legislator to make it happen, but it could have some interesting implications for the infrastructure.

Christelle Gloor: But how would you resolve conflicts there? What if someone has some AirTags on them that they would like to keep being tracked and then their neighbour on a tour bus for example, as has been said, has this track me not feature enabled?

Ross Anderson: The legislator decides. Were I the legislator, I would say that my right to privacy overrides your right to track with parliament. If we're all in the same space, we go to the parliament, we have the votes, we resolve it, conflict resolved.

Reply: There are false positives, yes. You could provide some feature which says we've detected that your tracker is being used for stalking and disabled it. If it is your tracker, you could put it within NFC range because Apple AirTags have NFC in them. So you can scan this with your phone to re-enable it. This forces you to get access to it again, rather than having it appear to be stalking somebody else.

Frank Stajano: So ultimately who has control over telling the tag what to do? What's the access control basically, or where should it be?

Reply: Apple controls it. Some people have done minor modifications like taking speakers out, but it would be the company that creates the trackers, that has the control.

Frank Stajano: But any of these things where you say, well Apple tell me to do that, only work if both the attacker and the victim are in the same technological ecosystem, right?

Reply: Yes, they are.

Frank Stajano: You can't really give these instructions to say, I don't want to be tracked if I get a Chinese brand.

Reply: Yes, exactly. So we would need it to be implemented across different operating systems. So we need Android to cooperate, but if we get Apple to do some features and then the victim has an Android phone, then that's one of the things that already exists, as a limitation where you have worse anti-stalking features.

Frank Stajano: The thing that makes me slightly uneasy about this is that you are talking about a collaborative solution to what is an adversarial setting. And so in the adversarial setting, the adversary, if it's an adversary, won't cooperate.

Reply: I think this is why it's nice to do it at the company or technological level. If the adversary is not going to cooperate, then we still have things built into these tracking devices to tell nearby other phones that they are following you.

Frank Stajano: If the adversary is someone who buys a tag from a company that does not want to play a game with Apple or Android or whatever because they just want to be, and I'm the stalker's friend who actually works, then you're not going to have much traction saying, Apple will then say blah blah because they're made on purpose for being the one that works. I mean like a poacher's friend will give you a trap.

Reply: The threat model we work with in the technology-based domestic abuser scenario is a "UI-bound adversary". They use tools and technologies entirely within the ways that you would expect normal users to use them. They're not going out of their way to create their own devices that can't be tracked or that aren't anything readily available that are made for stalkers at the moment. So what we're finding instead is people buying legitimate regular devices like the AirTag and Tile tracker and then misusing them rather than getting specialist devices on their own.

Frank Stajano: So I would argue, just for the sake of controversy, that it's nice to say if Apple made these things without the intention of them being used for stalking, it's nice if they fix it so that they cannot be used for stalking, when everybody's cooperating towards this laudable goal. But just in the way that there are things that are advertised for you and lets you track your partner and lets you stick that under the current and so on and so on. These people will see a market gap the more Apple fixes their thing and more say, now buy mine because I'm not going to listen to anything Apple says about not stalking.

Reply: Yes, that could potentially be a problem.

Andrei Serjantov: My question was going to be about threat models. Indeed, what is the threat model here? Is it that the device is on the side of the victim? Is it that iPhone is on the side, or the detector is on the side of the victim, et cetera? But actually, my question's going to evolve into is there any way of jamming these things?

Reply: Yes, it's Bluetooth so you can jam Bluetooth and you can interfere with it that way.

Andrei Serjantov: So that's much more adversarial, right?

Reply: Yes. It's also more technical, which again, we don't expect to be in the threat model of our scenario, but you could do if you want to.

Andrei Serjantov: But if I'm being a vulnerable journalist who's just released something super vulnerable, then my solution is not relying on Apple and all the other device manufacturers to have nice features in the thing. I need a jammer.

Frank Stajano: You're going to be followed by the fact that people see this cloud of jamming.

Andrei Serjantov: I don't care. In the end, my anonymity of a cloud of jamming is much better than a little coin tracking me. It means somebody would have to follow a cloud of jamming as opposed to sit in the cafe and go, okay, the BBC journalist goes from BBC to lunch to dinner and there's their home?

Ceren Kocaoğullar: So I have some questions about limiting the accuracy and providing false locations as protection measures. If you're talking about trying to find your keys in the house or keys in, you don't know where they are, maybe limiting the accuracy might be helpful in preventing you from finding your keys. But if you're talking about a person who has habits and patterns of movement, Maybe increasing the accuracy of their location from some metres to some kilometres might not be that helpful. Maybe for example, even if you changed the accuracy of my locations, you would just see if I'm in London or if I'm in Cambridge. And if I'm in Cambridge, if you know me, you're going to know where I'm going to be, in my college or in my accommodation. Same goals for providing false locations. I'm wondering what kind of mechanism you're thinking about because if this is something that's going to kick in once the stalking is the systems techs talking, then again a similar problem sort of might come up in that it just suddenly shows a different location for where I could be. But until then, if you could see that I was moving towards somewhere in Cambridge, then you can just connect the dots and say that she's in her student accommodation, or not.

Reply: So doing it subtly is hard. If you had a user who was very interested in intervening, you could perhaps have them provide chosen false locations for that version of it where you say, it looks like I'm going up the street, so I'm going to look like I'm going up Castle Hill when actually I'm going down Chesterton Road. This is a very Cambridge example. But perhaps the street splits at one point and I make it look like I'm going one way and may out to go the other. These don't provide quite real time location updates, I should say. It's whenever you pass nearby users, so it might be every two or three minutes, so not expecting to see the exact line up the street. They might see you are in Trinity College and now you are near the market somewhere, and then scattered locations around town. So you can give some amount of inaccuracy and it's still sensible.

Alex Shafarenko: I think there's a persistent assumption in all of that, that the communication is conducted via a mobile network or something, right?

Reply: Yes.

Alex Shafarenko: I think that's out of date now because you have Things Network, operate on LoRa, for instance. And it's a public network without authenticated entries. So any anonymous thing can actually log in and send messages and it is low power and it is long range. Also, there are various ideas, not just the one about jamming, which will be illegal. Because to reliably jam a Bluetooth signal, you have to radiate power several decibels, maybe 10, 15 decibels above the power of the source, which will break the law. But there are multiple public bands in the UHF area, which you can use legally and have long range communications. For example, family radio and you can actually send, you're talking about coordinates, right? So 60 bits, you can send it on a sound channel that people use for talking, right? And that'd be okay. So basically my conclusion from all of that is what Ross said, that without a legal framework, without making illegal stalking as such, not any kind of physical means of stalking, I don't think this game can be played successfully.

Reply: Okay, fair enough.

Anna Talas: So I don't actually think six hours is enough [when delaying location updates] because I have an AirTag and the way I mostly use it is did I take my keys with me? Are they with me right now? And if I, for example, left them on the bus before then I don't want to wait six hours to find out about that.

Reply: Yes. If it's in Bluetooth range of your current device, it'll say the thing is nearby, do you want to find it? And that's when it gives you the play a sound or use Bluetooth location options, rather than just finding it remotely. If it is something like you've left it on a bus, then that does break in that scenario. These are just ideas thrown out for things to do. We would appreciate suggestions for improvements while we're still trying to get the companies to respond to us.

Christelle Gloor: One other compromise could be that if you have this kind of situation where you really need to find something right now, the device starts to do some obnoxious sound that you need to turn off by actually pressing on the device. Because then if it's a stalking problem, it will just keep beeping until someone notices. But if it's just you missing your keys.

Reply: You can turn it off in the app as well.

Christelle Gloor: But that should not be possible, in my opinion.

Oliver Shapcott: I have a trivial question. On the analysis you did with the student society. You found that most of them didn't turn any functionality on. Could you maybe speak a bit about the makeup of the students you explored? Are they computer scientists? Are they people who are security aware? Could you give us a bit of background on that?

Reply: Yes. We put a demographics chart I put in the other paper we did on this. They are primarily undergraduate students, about two-thirds of which are sciences students, and then a mix in other subjects. Most of them have any prior experience of using trackers — one third had used them before, and one in ten used them regularly. A lot of them rated themselves as being technology competent. So they do think they know how to use this and three quarters of them were playing assassins for the first time. The rest of them had some experience with the game, so they're more experienced with doing this thing of hunting people down for sport.

Christelle Gloor: Are you considering redoing this game, but also training people explicitly in the beginning?

Reply: We could potentially do that. We wanted to not train them at all on any of this because we wanted to see how people looked for these things without giving them any extra information or prompting them to use the anti-stalking features and explicitly pushing them to use it. What we found actually was a lot of people just looking for things manually. We asked how'd you look for the tracker, and they said they looked under their bike seat before they got on it every day, or I checked my bag every evening. Or, oh, I forgot about it, were a couple of responses.

Christelle Gloor: I see the value of doing that if you're trying to figure out, if you're not aware of those trackers, are people going to be able to find that? But you might be able to find some different findings in terms of general usability, even if someone knows about those things, is it usable or not? Or if you see similar problems.

Reply: I think it would be good follow-on study.

Oliver Shapcott: You have over 80% though that aren't aware of the tracking features, would it be useful for these companies to make AirTag users, for example, aware that they can use find my or whatever it is to see that someone is actually tracking them?

Reply: They try to. If you have your own tracker, it gives you a bunch of information when you're setting up about finding these devices. They occasionally do little press releases and things about the features they've added. Mostly because again, there's loads of press coverage that Apple aren't doing it as well. Although I think Apple are doing better than the other companies we looked at in the study, they just get a lot of the negative press for it.