How criminals can steal your PIN by tracking the motion of your phone

April 10 2017

Credit: CC0 Public Domain

Hackers are able to decipher PINs and passwords just from the way we tilt our phone when we are typing in the information.

Cyber experts at Newcastle University, UK, have revealed the ease with which malicious websites, as well as installed apps, can spy on us using just the information from the motion sensors in our mobile phones.

Analysing the movement of the device as we type in information, they have shown it is possible to crack four-digit PINs with a 70% accuracy on the first guess - 100% by the fifth guess - using just the data collected via the phone's numerous internal sensors.

Despite the threat, the research shows that people are unaware of the risks and most of us have little idea what the majority of the twenty five different sensors available on current smart phones do.

And while all the major players in the industry are aware of the problem, no-one has yet been able to find a solution.

Publishing their findings today in the *International Journal of Information Security*, the team are now looking at the additional risks posed by personal fitness trackers which are linked up to our online profiles and can potentially be used to interpret the slightest wrist movements as well as general physical activities such as sitting, walking, running, and different forms of commute.

Dr Maryam Mehrnezhad, a Research Fellow in the School of Computing Science and lead author on the paper, explains:

"Most smart phones, tablets, and other wearables are now equipped with a multitude of sensors, from the well-known GPS, camera and microphone to instruments such as the gyroscope, proximity, NFC, and rotation sensors and accelerometer.

"But because mobile apps and websites don't need to ask permission to access most of them, malicious programs can covertly 'listen in' on your

sensor data and use it to discover a wide range of sensitive information about you such as phone call timing, physical activities and even your touch actions, PINs and passwords.

"More worrying, on some browsers, we found that if you open a page on your phone or tablet which hosts one of these malicious code and then open, for example, your online banking account without closing the previous tab, then they can spy on every personal detail you enter.

"And worse still, in some cases, unless you close them down completely, they can even spy on you when your phone is locked.

"Despite the very real risks, when we asked people which sensors they were most concerned about we found a direct correlation between perceived risk and understanding. So people were far more concerned about the camera and GPS than they were about the silent sensors."

Access without permission

Sensors are now commonplace in smart devices and are largely responsible for the boom in mobile gaming and health and fitness apps, and soon in all devices in the Internet of Things (IoT).

The data provided by them combined with the growing computational ability of mobile phones and tablets has transformed the way we use them.

In total, the team identified 25 different sensors which now come as standard on most smart devices and are used to give different information about the device and its user. Only a small number of these - such as the camera and GPS - ask the user's permission to access the device.

The study found that each user touch action - clicking, scrolling, holding and tapping - induces a unique orientation and motion trace. So on a known webpage, the team were able to determine what part of the page the user was clicking on and what they were typing.

"It's a bit like doing a jigsaw - the more pieces you put together the easier it is to see the picture," explains Dr Siamak Shahandashti, a Senior Research Associate in the School of Computing Science and co-author on the study.

"Depending on how we type - whether you hold your phone in one hand and use your thumb, or perhaps hold with one hand and type with the other, whether you touch or swipe - the device will tilt in a certain way and it's quite easy to start to recognise tilt patterns associated with 'Touch Signatures' that we use regularly.

"So the internal sensors each provide a different bit of the jigsaw. Personal fitness trackers which you wear on your wrist and, by their very nature, are designed to track the movement of your hand and pass information to your online profile pose a whole new threat.

"Potentially, they are able to provide additional information which, when combined with this sensor data, will make it even easier to decipher personal information."

So are we able to protect ourselves?

The team has alerted all the major browser providers - including Google and Apple - of the risks but for the moment, says Dr Mehrnezhad, no-one has been able to come up with an answer.

"It's a battle between usability and security," she says.

"We all clamour for the latest phone with the latest features and better user experience but because there is no uniform way of managing sensors across the industry they pose a real threat to our personal security.

"One way would be to deny access to the browser altogether but we don't want to lose all the benefits associated with in-built motion sensors."

As the result of the research, some of the mobile browser vendors such as Mozilla, Firefox and Apple Safari have partially fixed the problem, but for an ultimate solution, the Newcastle team is still working with industry.

Dr Mehrnezhad, who together with her colleague and co-author Ehsan Toreini run the Cyber Security: Safety at Home, Online, In Life course, part of Newcastle University's series of MOOCs (Massive Open Online Courses), say there are some simple rules people should follow:

- Make sure you change PINs and passwords regularly so malicious websites can't start to recognise a pattern.
- Close background apps when you are not using them and uninstall apps you no longer need
- Keep your phone operating system and apps up to date
- Only install applications from approved app stores
- Audit the permissions that apps have on your phone
- Scrutinise the permission requested by apps before you install them and choose alternatives with more sensible permissions if needed

More information: Stealing PINs via Mobile Sensors: Actual Risk versus User Perception. Maryam Mehrnezhad, Ehsan Toreini, Siamak Shahandashti and Feng Hao. IJIS - *International Journal of Information Security* - (10207/IJIS)

More information on how to stay safe can be found here: www.futurelearn.com/courses/cy … urity/2/steps/160839

Provided by Newcastle University