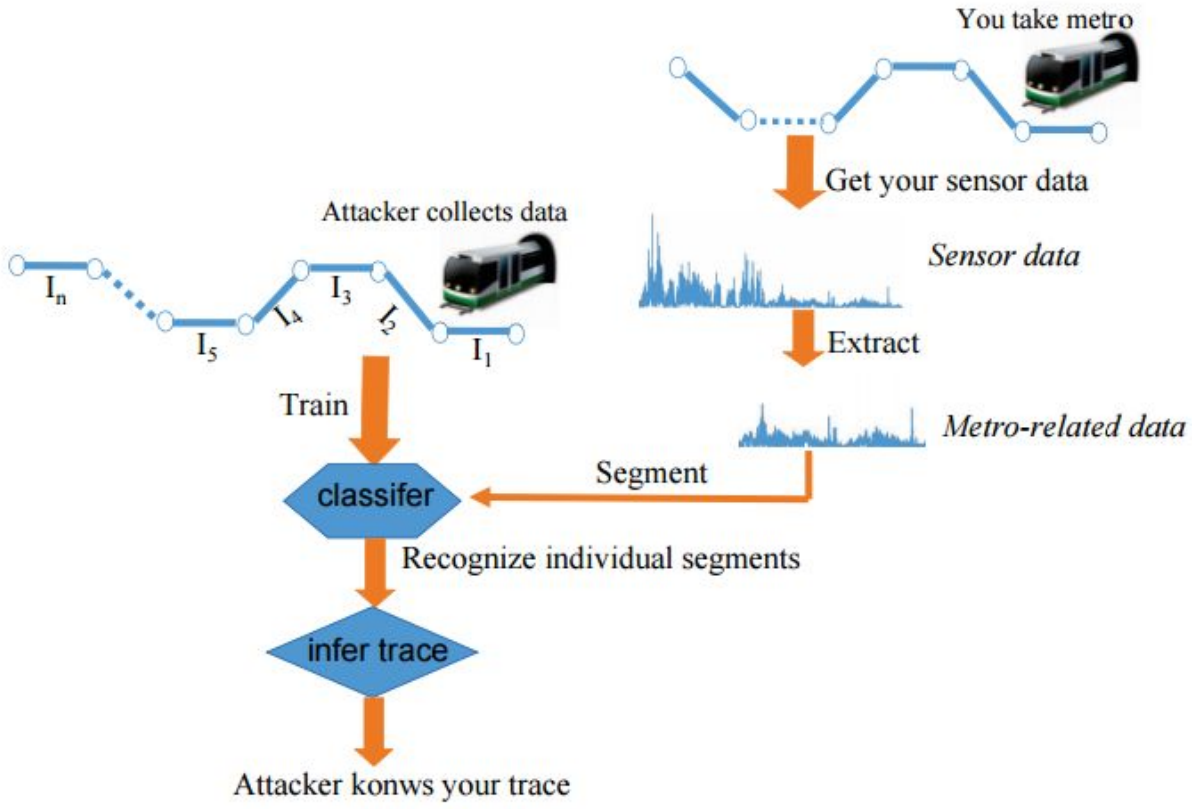
Subway riders' smartphones could carry tracking malware

May 26 2015, by Nancy Owano



Attack model. Credit: arXiv:1505.05958 [cs.CR]

Millions of city dwellers with smartphones in hand, pocket or bag, use trains to get around night and day, seven days a week. The incoming message from three researchers in China is that an attacker could track

them based on information from a phone's accelerometer. The three, from Nanjing University, have completed a study which went up on the arXiv server earlier this month. "We Can Track You If You Take the Metro: Tracking Metro Riders Using Accelerometers on Smartphones" describes the attack.

Patrick Howell O'Neill in the *Daily Dot*, said the research was about an " attack that learns each subway's fingerprint and then installs malware on a target's phone that steals accelerometer readings."

No GPS is involved in this type of attack, which works underground. (The authors said that "metro trains often run underground, where GPS is disabled.") They said that if "a person with a smartphone takes the metro, a malicious application" uses accelerometer readings to trace the person, to infer where the victim gets on and off the train. They said that "metro trains run on tracks, making their motion patterns distinguishable from cars or buses running on ordinary roads."

It is possible, they wrote, "that the running of a train between two neighboring stations produces a distinctive fingerprint in the readings of 3-axis accelerometer of the mobile device, leveraging which attackers can infer the riding trace of a passenger."

The researchers raised three concerns. First, it's easy for attackers to create stealthy malware to eavesdrop on the accelerometer. Second, the metro, they said, is the preferred transportation means for most people in major cities. The last point is that metro-riding traces can be used to further infer other private information. "For example, if an attacker can trace a smartphone user for a few days, he may be able to infer the user's daily schedule and living/working areas and thus seriously threaten her physical safety." What is more, an attacker may find that two individuals often visit the same stations, they said, at "similar non-working times," and may infer a relationship.

The Nanjing University trio said that they were "the first to propose an accelerometer-based side channel attack for inferring metro-riders' traces."

They conducted their experiment on a Nanjing metro line. They found that the inferring accuracy reached 92 percent if the user took the metro for six stations.

Could one tell or at least suspect if such malware were operating in the background? O'Neill said one interesting defense against such a hack would be to scrutinize the phone's power consumption. "To track someone using this method, a hacker would have to continuously access the phone's accelerometer, draining significant power no matter how well the malware was concealed," he said. By monitoring the phone's power consumption, one may see when an app is using too much of the battery.

The authors said that "If malware intends to steal the users' privacy through sensor data, constant request for the data from sensors will evidently boost the power consumption. No matter how the malware tries to conceal itself, the acquisition of sensor data will lead to an increasing power consumption of the smartphone."

More information: We Can Track You If You Take the Metro: Tracking Metro Riders Using Accelerometers on Smartphones, arXiv:1505.05958 [cs.CR] arxiv.org/abs/1505.05958v1

Abstract
Motion sensors (e.g., accelerometers) on smartphones have been demonstrated to be a powerful side channel for attackers to spy on users' inputs on touchscreen. In this paper, we reveal another motion accelerometer-based attack which is particularly serious: when a person takes the metro, a malicious application on her smartphone can easily

use accelerator readings to trace her. We first propose a basic attack that can automatically extract metro-related data from a large amount of mixed accelerator readings, and then use an ensemble interval classier built from supervised learning to infer the riding intervals of the user. While this attack is very effective, the supervised learning part requires the attacker to collect labeled training data for each station interval, which is a significant amount of effort. To improve the efficiency of our attack, we further propose a semi-supervised learning approach, which only requires the attacker to collect labeled data for a very small number of station intervals with obvious characteristics. We conduct real experiments on a metro line in a major city. The results show that the inferring accuracy could reach 89% and 92% if the user takes the metro for 4 and 6 stations, respectively.