Easy prey for hackers—navigation systems

January 25 2016

When it comes to route planning, drivers have almost blind faith in GPS; the technology plays a crucial role in identifying location and time in the industry as well as in other areas. If hackers attack the system, they can cause great damage. Deploying several GPS receivers at the same time could solve the problem in certain areas of application.

Fake signals appear authentic

If an attacker wants to manipulate the GPS, he can use a satellite simulator for the purpose. That device generates fake satellite signals that appear authentic, and sends them out to receivers such as the satnav in the car. "This is how attackers can fool the receiver, which then assumes it is located in a different position than is actually the case," explains Jun. Prof Christina Pöpper, who heads the work group Information Security at the Horst Görtz Institute and is developing a solution to the problem together with her PhD student Kai Jansen. The industry can be affected as well, because here, GPS is utilised for temporal synchronisation of machines. Production might come to a standstill due to manipulation.

Several receivers instead of one

When proposing their solution, Christina Pöpper and Kai Jansen considered what happens when a vehicle or a machine uses not one, but several receivers at the same time, which are situated at a distance from each other. If they receive genuine satellite signals, the receivers' calculated positions differ slightly from each other. If, however, an

attacker transmits signals using a simulator, they appear deceptively authentic and are identical for each individual receiver. The attack can only be detected by comparing the individual receiver positions to each other, because now all receiver devices believe to be in the same wrong position. This is because the relative reception times of several signals which are transmitted via the satellite simulator are identical in several receiver devices. This is not the case when legitimate satellite signals are received, because they are transmitted from different positions in earth orbit.

Two to three metres between the receivers

"We have already demonstrated that this is how we can detect attacks," says Christina Pöpper. "At present, we are figuring out technical details. Details such as the minimum distance that is required between the receiver devices to make sure that they don't identify their positions as identical when receiving authentic signals due to inaccuracies that will inevitably occur." According to the latest findings, the minimum distance between the devices should range between two and three metres. If the receivers are closer together, the error rate increases. "This can be easily realised in large vehicles or machines, such as trucks or ships, because here the receivers can be positioned at a sufficiently great distance from each other," says Pöpper. "A solution for mobile phones or other devices that are spatially restricted still needs to be found."

More information: Raffaela Römer , "Easy prey for hackers: navigation systems. Make a U-turn when possible", RUBIN Science Magazine, ISSN 0942-6639. rubin.rub.de/en/easy-prey-hack … s-navigation-systems

Provided by Ruhr-Universitaet-Bochum

Citation: Easy prey for hackers—navigation systems (2016, January 25) retrieved 28 June 2024 from https://phys.org/news/2016-01-easy-prey-hackers.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.