

Researchers successfully hack into automobiles using passive keyless systems

January 7 2011, by John Messina



Attacker starts a car using an antenna. A signal from the car is transmitted to a computerized key, which is tricked into enabling the engine ignition.

Credit: ETH Zurich

(PhysOrg.com) -- Researchers at a system security group at ETH Zurich in Switzerland were able to access ten automobiles from eight manufacturers and drive them away.

A passive keyless entry system is activated when a wireless key is within a few meters of the correct automobile and detects a low power signal from the vehicle. The wireless key then sends a command that opens the vehicle and starts the ignition.

Srdjan Capkun, an assistant professor of computer science, along with his colleagues, managed to intercept and relay signals from the vehicle to their wireless keys. They could have also relayed the signal from their wireless key back to the vehicle, but choose not to because the key can transmit its signal up to 100 meters (approx 328 feet). Their attack proved successfully no matter what cryptography and protocols the key and vehicle used for communication.

The attack was carried out by using a pair of antennas to transmit signals from the vehicle to the wireless key when the key was far away, tricking the vehicle into opening and starting. One antenna needs to be very close to the automobile while the other needs to be within eight meters of the key.

Most relay attacks require the signal to be converted from analog to digital and back to analog again causing delays in microseconds. These delays can cause the vehicle not to open or start. This was circumvented by keeping the signal in analog format, cutting the delay down to nanoseconds.

There's not too much automobile owners can do to protect themselves except for maybe shielding their wireless key when leaving their vehicle. Capkun says manufactures will need to add secure technology that allows the vehicle to confirm that the wireless key is close by. The researchers are actively working on protocols that would make this happen.

More information: Via: [Technology Review](#)

© 2010 PhysOrg.com

Citation: Researchers successfully hack into automobiles using passive keyless systems (2011, January 7) retrieved 26 April 2024 from <https://phys.org/news/2011-01-successfully-hack-.html>

[automobiles-passive-keyless.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.