

REMOTE START SYSTEMS - FRIEND OR FOE?

A Transponder-equipped vehicle's security is not compromised by a correctly installed remote start system. The important word here is correctly - as that is not always the case in our experience.

After-market remote start systems typically allow temporary engine operation by Remote activation of their own hard-wired, parallel, normally dormant, transponder/antenna circuit. When their Remote transmits the appropriate RF signal to a receiver in the surrogate circuit, a Relay (electric switch) completes a circuit which temporarily replicates the vehicle's own transponder/antenna circuit - in effect tricking the vehicle's ECU into allowing an engine start by duplicating essential conditions. The critical words here are temporary, dormant and parallel! None of these systems allow moving operation without a working transponder key in the ignition lock as they are designed to return to a dormant status if the brake pedal is touched or the transmission is shifted out of Park.

Components of a typical Remote Start System's parallel circuit include an antenna/induction coil, a plastic key box, a receiver, relays and/or an integrated circuit with proprietary logic.

The vehicle owner must provide a working transponder key for installation in the key box. What is critical here is that the blade section of the key must be defaced, cut entirely off or left blank. Under no circumstances should a complete working key be placed in the key box - but we have encountered several situations where they were.

The parallel circuit can only be activated by its own remote transmitter and becomes dormant if the vehicle's hood is opened, by the first tap of the brake pedal or by an attempt to operate the car by shifting out of Park!

We feel that a correctly installed Remote Start System's only vulnerability lies with the configuration of the transponder key installed in the system's key box.

Portable scanners are not a factor in our experience. A scanner may be capable of intercepting, recording and duplicating a nearby Remote's RF transmission - a factor that might put your garage door opener at risk, but does not degrade the security of a Remote Start System due to their capability of shutting down if the brake pedal is touched or the transmission is shifted out of Park.

Interception of the hidden transponder's output by scanning is not a practical consideration as its field of vulnerability is 2mm - an area roughly the size of a Ping Pong ball.

Anthony Sabetti of Texas Instruments has reported that 12 inches is the greatest distance his company's engineers have managed to intercept a transponder's output, and then only that in the laboratory with large antennas that require a power source.

There is no question that the installation of a remote start system in a transponder equipped vehicle compromises the system if the installer places a complete, correctly cut key in the box under the dash under the dash key - but only if the key is removed from the box and used in the ignition - within 2mm of the original, undamaged induction coil.

Most systems also have a feature that will prevent starter engagement while the engine is already running - because you have to turn the ignition switch on with a working transponder key when you enter the car after you have remotely started it.

We have also encountered situations where a correct resistor was hard wired in series into a PASS-VATS system - completely disabling it - to allow remote starting.

We recommend an inquiry concerning specifics of a remote start system during a routine post-theft interview as it may be as important to your investigation as obtaining the owner's transponder keys.

E. McCabe - 2004