High Tech Auto Theft

By Daryl Allegree, CSP, ARM
Zurich Resilience Solutions | Risk Engineering

According to the U.S. Department of Justice, vehicle thefts were up 11.8% from 2019 to 2020* and the trend appears to have continued during 2021. The global pandemic may be contributing to the increase in thefts. According to David Glawe, President and CEO of the National Insurance Crime Bureau, "there is high demand for used vehicles, and low supply. That makes for a perfect storm for increased crime".

The New York Police Department and New York Attorney General announced a successful conclusion to their investigation dubbed 'Operation Master Key'. An auto theft ring responsible for over 225 vehicle thefts was taken down and 10 suspects were charged with multiple crimes. The Commissioner of the NYPD said, "This was a complex, high-tech operation that sought to weaponize every hidden vulnerability in the automotive industry, from creating keys based on bootleg code lists, to altering computer settings, to creating a mill that furnished false registrations for altered VINs.

Technology has been a boon to automakers and consumers. Everything from adaptive cruise control, to automated emergency braking and forward collision warning systems, have made the driving experience better, and safer. However, advancements in technology can have a downside. Keyless entry and ignitions are very convenient for drivers, and maybe equally convenient for thieves. In many cases it's extremely easy to access a vehicle. If the driver inadvertently leaves the key fob inside the car, someone can just walk right up, open the door, and drive off. In other cases, the thieves must be clever and well equipped.

High Tech Theft

Today's car thieves need help to overcome and defeat vehicle security systems. 'Relay attacks' take advantage of vulnerabilities in keyless entry systems. Two thieves work in tandem using devices that pick up the key fob signal from inside a building, and then amplify it. One person stands next to a building (make ready or detail shop for example) and their device picks up a key fob signal from inside. That signal is amplified and then relayed to the second individual who's standing by the vehicle's car door with another device. The vehicle thinks the key fob is there, so the door can be opened, and the ignition activated.

A second, high-tech method is gaining in popularity due to improved vehicle security systems – it is much more difficult to steal a car without a key/fob. On-Board Diagnostics (OBD) ports are being exploited by thieves to access vehicle ignition systems. They use force to break windows and enter the vehicle to link up with the OBD port, then connect a professional grade programming tool to the port and "program" a new key fob.

Both the tools and key fobs are readily available on the internet or can be stolen from legitimate users like locksmiths or auto service facilities. Once the new fob is programmed the thieves fire up the engine and drive off with their prize.

An ounce of prevention

So, what can dealerships and consumers do to protect their vehicles? Layered security is the best option for auto dealers. Seal the lot perimeter using fencing, gates, blockers and natural terrain features like ditches and trees. Installing active video monitoring systems that include motion-activated cameras and are monitored 24/7 offers excellent protection. High value and targeted inventory should be stored inside or in other protected areas.

Other security options include:

- Lock the doors and take the keys
- Equip all buildings with alarm systems that are monitored by a central station
- Install an OBD lock to prevent thieves from accessing the port
- Use a steering wheel lock as a mechanical deterrent
- Install an immobilizer or other aftermarket anti-theft system
- Aftermarket alarm systems in addition to the OEM product
- GPS asset tracking systems to alert dealership personnel whenever the vehicle moves and provide geo-fencing features
- Store keys in Faraday Bags or sealed metal containers to block key fobs from transmitting codes outside the building

Eventually, manufacturers will need to address vulnerabilities in keyless systems and come up with solutions to protect vehicle owners. Dealers should consult with local law enforcement to determine which vehicles (or manufacturers) are being targeted in their region. If specific vehicles are being stolen, add an extra layer or two of security to those vehicles. Many cities have vehicle anti-theft task forces or similar units that may be a good source of information and can offer additional prevention strategies.

Zurich
1299 Zurich Way, Schaumburg, Illinois 60196-1056
800.382.2150 www.zurichna.com