Texting, grand theft auto style; alarms pose risk

August 19 2011, By JORDAN ROBERTSON , AP Technology Writer

In this photo taken Tuesday, Aug. 16, 2011, security consultants Don Bailey, left, and Mathew Solnik, right, with iSEC Partners, demonstrate with a computer how they force cars with certain alarm systems to unlock their doors and start their engines by sending them text messages in San Francisco. (AP Photo/Eric Risberg)

Texting and driving don't go well together - though not in the way you might think.

Computer hackers can force some cars to unlock their doors and start their engines without a key by sending specially crafted messages to a car's anti-theft system. They can also snoop at where you've been by tapping the car's GPS system.

That is possible because car alarms, GPS systems and other devices are increasingly connected to cellular telephone networks and thus can receive commands through text messaging. That capability allows owners to change settings on devices remotely, but it also gives hackers a way in.

Researchers from iSEC Partners recently demonstrated such an attack on a Subaru Outback equipped with a vulnerable alarm system, which wasn't identified. With a laptop perched on the hood, they sent the Subaru's alarm system commands to unlock the doors and start the engine.

Their findings show that text messaging is no longer limited to short notes telling friends you're running late or asking if they're free for dinner.

Texts are a powerful means of attack because the devices that receive them generally cannot refuse texts and the commands encoded in them. Users can't block texts; only operators of the phone networks can.

These devices are assigned phone numbers just like fax machines. So if you can find the secret phone number attached to a particular device, you can throw it off by sending your own commands through text messaging.

Although these numbers are only supposed to be known by the devices' operators, they aren't impossible to find. Certain network-administration programs allow technicians to probe networks to see what kinds of devices are on them. Based on the format of the responses, the type and even model of the device can be deduced. Hackers can use that information to craft attacks against devices they know are vulnerable. (In this case, the researchers bypassed these steps and simply took the alarm system out of the car to identify the secret phone number.)

Actually stealing a car wouldn't be so easy.

You'd have to ensure that the phone number you found is attached to the car you're standing in front of, for instance. There are hacking tools to do that - they listen for cellular traffic around a particular vehicle - but in many cases it's easier to take a car that doesn't have an alarm.

The research from Don Bailey and Mat Solnik is unsettling because it shows that such attacks are possible on a variety of other devices that use wireless communications chips. Those include ATMs, medical devices and even traffic lights. Hackers have already sent specially crafted texts with commands to instantly disconnect iPhones from the cellular network.

Bailey, whose specialty is cellphone network security, also found that similar techniques can be used to get a certain type of GPS system to cough up its location data. Such information can be used by stalkers or home burglars, for instance.

The type of GPS system he studied is known as assisted GPS, which means that it uses cellular signals in addition to the usual satellite signals. That makes the system vulnerable.

The research isn't just about taking off with someone else's car or finding out where that person has been.

It raises the possibility of other, more sinister dangers, such as those potentially affecting braking and acceleration, said Scott Borg, director of the U.S. Cyber Consequences Unit, a group that studies hacking threats. That becomes possible as networked electronics are more tightly coupled with physical machinery.

"Doing one that is harmful is quite hard, but we need to prepare for people doing that," Borg said.

The research got the attention of a trade group for electric utilities, the North American Electric Reliability Corp. After the pair showed off the techniques at the Black Hat security conference in Las Vegas this month, the group warned that the types of wireless chips exploited by the pair are also used at power plants and said that more caution is needed in their use.

The vulnerable GPS system was made by Zoombak Inc., which promotes its products' usefulness in tracking children and automobiles. The company said it has made changes to its devices, so that outside parties can no longer get location data without passwords.

Bailey and Solnik are working with the manufacturer of the car alarm system to fix its vulnerabilities. Bailey said the unidentified manufacturer has fixed many of the security issues.

Bailey said stricter security standards are needed.

"We're so excited to use technology that we're deploying it too quickly and not really thinking about the impact of security," he said.

Citation: Texting, grand theft auto style; alarms pose risk (2011, August 19) retrieved 26 April 2024 from https://phys.org/news/2011-08-texting-grand-theft-auto-style.html