

Search CNET

Reviews

News

Video

How To

Download

US Edition

CNET > Security > Personal-safety GPS device presents security risk

Personal-safety GPS device presents security risk

Locator device can help you find your stolen car or keep track of your kids, but it can also beam information to would-be miscreants, researcher says.

by **Elinor Mills** @elinormills / April 22, 2011 12:49 PM PDT

0 / 0 / 0 / 0 / / more +

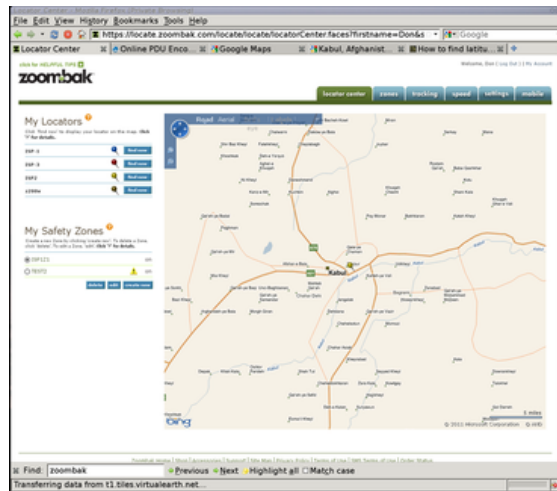
After thieves tried several times to steal a friend's car, Don A. Bailey bought a Zoombak personal GPS Locator device so that if the thieves ever succeeded, the car's owner would be able to track its whereabouts and get it back.

He never got to try it out on a theft, but Bailey hacked the device and learned that by exploiting security weaknesses in it, he could monitor the movements of a known device, impersonate it to the Zoombak tracking system, and even look for devices in his immediate vicinity to target.

The potential for abuse is not insignificant given that the device is marketed as a safety device—a way to keep track of the whereabouts of things that people might steal or harm, like **cars**, bikes, pets, and even children.

"You assume that this device is adhering to the security guarantees they're making, to keep children safe by allowing parents to know where they are at all times," Bailey, a senior security consultant at **iSec Partners**, said in an interview with CNET today. "But I can locate where the device is and trick you into believing that the information about its location that is being provided is true when it's not."

It's unknown how many people use Zoombak devices. The company has said in marketing materials that it has shipped tens of thousands of devices and that they're sold in 13,000 stores nationwide, including Best Buy.



Bailey was able to trick the Zoombak system into believing a device in his possession in the United States is actually in Afghanistan.

Don A. Bailey

THIS WEEK'S MUST READS /

- 1 **Personal-safety GPS device presents security risk**
Security
- 2 **Dear Microsoft: Why does Outlook 2013 cost \$110?**
Software
- 3 **Apple defended iPod from hackers, iTunes chief says in antitrust trial**
Digital Media
- 4 **Sony hack leaked 47,000 Social Security numbers, celebrity data**
Security
- 5 **Tim Cook's name to grace Alabama antidiscrimination bill**
Tech Culture

Bailey couldn't say whether other GPS location devices are secure because he didn't look at any others. But he speculated that if the market leader, with top-notch engineering in all other aspects, is susceptible, it's quite possible other GPS tracking devices are as well.

"It's the most robust consumer tracking device on the market, and there's nothing else available that has its usability and features," he said.

Bailey said he tried to notify Zoombak about the problems, but was never able to get someone to address his concerns despite repeated e-mails and phone calls. The parent company (Securus recently acquired Zoombak) referred him to Zoombak customer support when he called. Zoombak's site refers media queries to Securus, which did not return an e-mail and phone call seeking comment today.

Trustworthy?

In a video ad on the **Zoombak Web site**, the palm-size, \$99 tracking device provides parents peace of mind when their daughter drives off to college by herself. In other marketing materials on the site, the eSafe version is seen attached to the backpack of a child boarding a school bus, the eCare version is focused on the elderly, and SpotLite is used for pets. The device has even been given the Oprah blessing, listed at No. 16 in O Magazine's **"100 Things That Are Getting Better"** article ranking what it considered "bright spots on the horizon" last year.

But can you trust the gadgets? For most uses, probably. But if what you are protecting is something that criminals might want to locate, and you really want to be safe, you might want to go with a bodyguard instead. Here's why:

Zoombak devices communicate with the Zoombak servers over SMS and GPRS (General Packet Radio Service), providing information about where the device is at any given time. The device uses satellite-based Global Positioning System data, including latitude and longitude, like car navigation and smartphones do. But unlike the iPhone, which **was found** to be logging and storing location data unencrypted on the devices without user permission, this data is not stored locally and is necessary for the tracking services that the device owners are seeking.

Technically, it's an Assisted GPS (A-GPS) device, because it combines the GPS data with location data from cell towers and transmits it to a remote server where a database translates the information into a physical location. The owner of the device can view the location on a map by logging into the Zoombak site and be notified if it reaches a specified destination or see where a stolen bike or car is that has a device attached.

Bailey, an expert in **telecommunications snooping**, was able to figure out that there is no authentication used when the device communicates with the manufacturer's servers, and he was able to intercept the messages. This allowed him to impersonate the manufacturer and find out where the device was, as well as feed false location information from the device back to the Zoombak servers.

"Once I had the device compromised, I was able to take out the SIM card and spoof messages to the manufacturer," said Bailey, who has proved that the attacks work and gave a presentation on his research at the Source security conference in Boston yesterday.

"It was a lot simpler than I thought it was going to be," he said. "People who are familiar with GSM (Global System for Mobile Communications), GPRS, and embedded devices in general are probably going to be able to compromise the device much faster than I did."

But in a real-world scenario an attacker may not have physical access to the target device. Bailey figured out a way to scan the telephone network to look for random Zoombak devices that might be close by. The technique involves discerning the patterns the locator devices use for sending and receiving messages over cellular networks and finding patterns that match those to home in on.

Bailey first did device profiling to narrow down the possible set of phone numbers to try. Potential numbers are only on T-Mobile because the devices only use that service, and they are not associated with a particular person, so they wouldn't be in the Caller ID database, he said. Armed with a subset of numbers based on those criteria, an attacker could send SMS messages to those and see which respond as a Zoombak would.

"If I query thousands of phone numbers across the U.S. and analyze them for their fingerprint, I can determine if they are a close match to my target (type of) device, and if so then send a forged SMS message (pretending to be Zoombak) and a fair percentage of numbers will respond as that type of device," he said.

"Now I can find the car you are worried about me stealing, or the pharmaceuticals traveling across the U.S., or track your child walking to school," Bailey said. "With my ability to constantly poll these devices over time I always know where they are."

Though an attacker wouldn't know exactly what valuable asset was attached to the device located, that information could be inferred based on details of the locations the device visits and the travel patterns. For instance, a device that is tracked moving from a residence every morning at the same time to the location of a grade school and back again at the same time every afternoon could indicate that it is located in the backpack of a student, he said.

An attacker "can now track assets which are tied to the physical world," he said. "This is very scary."

Tags: Security, Tech Culture

FEATURED VIDEO



SOFTWARE

Apple working on new "drop system" to save your iPhone

A new patent reveals Apple's plans to prevent your iPhone from falling on its screen. Puported iPad Pro schematics are revealed and Steve Jobs still has his swagger. / [WATCH VIDEO](#)

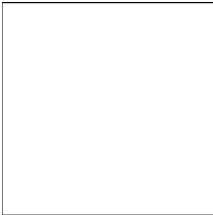
ABOUT THE AUTHOR



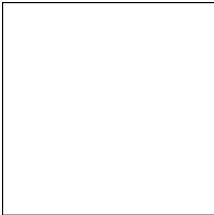
Elinor Mills /

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. [E-mail Elinor](#). [See full bio](#)

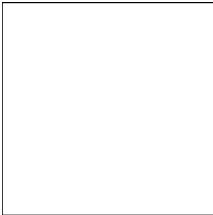
YOU MAY ALSO LIKE



Best iPhone 6 and iPhone 6 Plus cases - CNET - Page 44



A home air purifier with a cool twist -- cold plasma - CNET



Video captures pilot landing plane sideways in fierce winds - CNET

Learn more

Powered by

for Anna

JOIN THE DISCUSSION

0 Comments / 1 person following

Log In

+ Follow conversation

Share

Post Comment As...

Show Comments

LATEST GALLERIES FROM CNET

Orion's maiden voyage full of fire and space (pictures)

The 1,035-horsepower hybrid Ferrari FXX K is obscenely exotic (pictures)

Monday Night Tablet: Close-up with an NFL Surface tablet (photos)

Inside an Emirates A380 (pictures)

Osram's 40W Replacement Ultra LED shines (pictures)

Eye-catching McLaren 650S Spider uses race-bred tech (pictures)

REVIEWS	NEWS	VIDEO	MORE	FOLLOW CNET VIA...
All Reviews	All News	All Video	About CBS	Facebook
Audio	Apple	Apple Byte	Interactive	Twitter
Cameras	Crave	CNET On Cars	About CNET	Google+
Car Tech	Internet	CNET Top 5	CNET 100	YouTube
Desktops	Microsoft	CNET Update	CNET Deals	LinkedIn
Laptops	Mobile	Next Big Thing	CNET Forums	Tumblr
Phones	Sci-Tech	The 404	CNET Magazine	Pinterest
Tablets	Security	The Fix	CNET Mobile	Newsletters
TVs	Tech Industry	XCAR	Help Center	RSS
			Permissions	

