Thwarted by the iPhone, code-breakers turn their attention to other products

March 11 2016, by Paresh Dave, Los Angeles Times

Computer hacker Will Strafach had no trouble seizing control of the original iPhone. Same went for later generations over the next five years.

But by now, Apple Inc. has introduced so many layers of protection inside its flagship device that Strafach and others have moved on. As the frenzied hacking has subsided, publicly shared solutions to crack iPhone security are becoming harder to come by.

The frustration he and other hackers felt has hit law enforcement too. That's why agencies around the country say Apple is its last hope to unlock hundreds of smartphones important to investigations, and why the FBI is so forcefully going after Apple in its effort to get into the work iPhone of San Bernardino terrorist Syed Rizwan Farook.

Whereas a generation of hackers grew up tinkering with iPhones and Androids for fun, today's up-and-comers - thwarted by the near-ironclad security of smartphones - are shifting their focus to virtual reality headsets, self-driving cars, the cloud, mobile apps and other emerging online systems with less-tested locks.

Hackers like Strafach are instrumental in rooting out vulnerabilities in software and hardware. Their findings are used by specialty technology companies to design tools that extract and analyze data from devices, which are in turn used by law enforcement, technical consultants for attorneys and repair shops.

Nowadays, the more difficult task of smartphone hacking is falling to large, more well-financed teams at cybersecurity firms and secretive government departments, all of which are prone to closely guarding those vulnerabilities for national security reasons rather than sharing them with police.

"The better technology gets, the more rarefied and the smaller pool of true old-school hackers you'll have," said Greg Buckles, co-founder and principal analyst of forensics industry research firm EDJ Group.

IPhone software developer Ryan Petrich said he expects hobbyists to be outgunned within the next two years.

"It will be infeasible to develop an exploit outside a large team with very experienced security researchers," he said. "They will do things like attack specific parts of the system, but you aren't going to see ... full system access."

Strafach was a big part of the iPhone jailbreaking community, which finds holes in the iPhone operating system that can unleash unauthorized privileges.

For example, Apple allows installation of only apps it approves. A jailbroken phone eliminates the restriction.

The downside is that jailbreaking risks corrupting the phone permanently if the technical process goes awry. And demand for jailbreaking tools relaxed as iPhones began to include some of the functionality once available only on jailbroken devices.

As a teenager, Strafach would trade jailbreaking tips with about 10 buddies - the Chronic Dev team - in a private online chat room. They'd share their findings for others to use.

Jailbreaking tools have been "bit-for-bit critical" for forensics software makers to provide easy ways to read the contacts, messages, app data and other information on smartphones, he said.

Getting into the first-generation iPhone, released in 2007, was easy - Strafach compares it with finding a loose brick in a wall.

But the time he and his collaborators spent looking for loose bricks increased with each new iPhone and iPhone operating system - and there were additional hurdles.

It was as if the prize they were after was now also protected by cannons, a moat filled with alligators and a chain-link fence. To make matters worse, software updates would change the order and strength of obstacles.

By iOS 7 in 2013, the multilayered defense was overwhelming. Apple went "wild," over-securing systems "that didn't need more security," Strafach said.

He went on to start Groton, Conn.-based Sudo Security Group Inc., which is developing software for businesses to control which apps employees may download onto their mobile devices.

Nowadays, hackers can generally get only a piecemeal view into the iPhone. There is scanning software as well as passcode-guessing gadgets that can get some data from newer iPhones that are locked and running iOS 8 or iOS 9.

But no publicly known process can extract their entire contents the way they could on earlier operating systems.

One upside, Strafach said, is that the dried-up market "makes me feel

safe to have an iPhone."

Strengthened mobile device security has been a major force holding back growth of the forensics-tools industry.

Other jailbreakers left for technology companies as they aged, typically driven off like Strafach by a variety of reasons - stronger security among them. Others like George Hotz, who's developing a self-driving car, are getting ahead of tech's next big trends.

Jailbreaking remains big in China, where technology giants and advertisers sponsor efforts, labor costs are lower than those in the U.S. and demand for the pirated content available through unauthorized apps is incredible.

But security concerns and language barriers make their tools less viable outside of China.

Others haven't given up. Irvine-based Susteen Inc. dedicated several employees to uncovering vulnerabilities in iOS 9, spokesman Jeremy Kirby said.

And the company is actively looking to pay outside researchers for ideas.

British tools shop Fonefun has turned to makeshift solutions, like taping down the power button on iPhones, tearing open the device and soldering in new wiring to overcome restrictions on passcode-guessing.

"It's all about persevering until you find something that works," said Fonefun's Mark Strachan. "And hopefully we can get something positive out of that before Apple releases a new iOS and closes it."

Since iOS 9 debuted in September, Apple already has addressed more

than 70 security issues through updates, according to mobile security provider NowSecure. Such figures give experts confidence that there always will be a way in.

But they acknowledge the only surefire way to penetrate Apple's top security measures is to get a hold of the company's digital stamp, which is what the FBI is seeking in the San Bernardino terrorism investigation.

Otherwise, "law enforcement is kind of in a pickle," Petrich said.