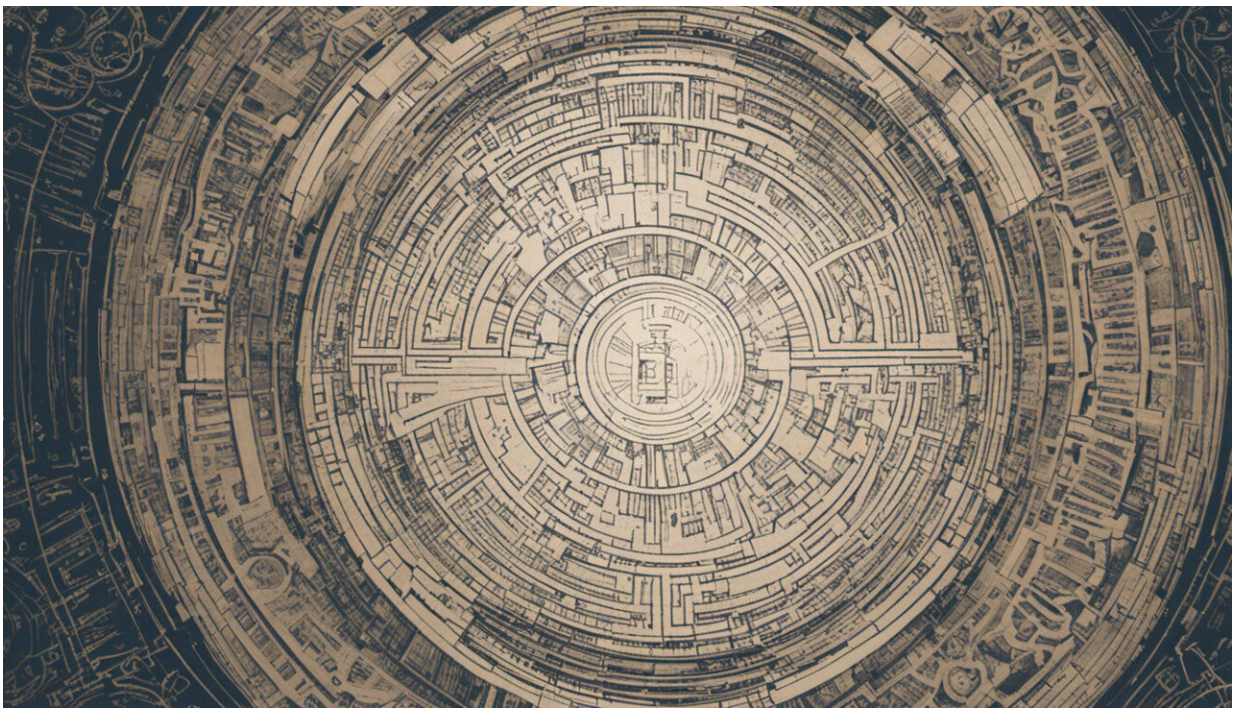
Bypassing encryption: 'Lawful hacking' is the next frontier of law enforcement technology

March 17 2017, by Ben Buchanan



Credit: AI-generated image (disclaimer)

The discussion about how law enforcement or government intelligence agencies might rapidly decode information someone else wants to keep secret is – or should be – shifting. One commonly proposed approach, introducing what is called a "backdoor" to the encryption algorithm

itself, is now widely recognized as too risky to be worth pursuing any further.

The scholarly and research community, the technology industry and Congress appear to be in agreement that weakening the encryption that in part enables information security – even if done in the name of public safety or national security – is a bad idea. Backdoors could be catastrophic, jeopardizing the security of billions of devices and critical communications.

What comes next? Surely police and spy agencies will still want, or even need, information stored by criminals in encrypted forms. Without a backdoor, how might they get access to data that may help them solve – or even prevent – a crime?

The future of law enforcement and intelligence gathering efforts involving digital information is an emerging field that I and others who are exploring it sometimes call "lawful hacking." Rather than employing a skeleton key that grants immediate access to encrypted information, government agents will have to find other technical ways – often involving malicious code – and other legal frameworks.

Decades of history

In the mid-1990s, the Clinton administration advanced a proposal called the Clipper Chip. The chip, which ultimately was doomed by its technical shortcomings, was an attempt to ensure government access to encrypted communications. After the chip's introduction and failure, a group of cryptographers formally studied various mechanisms that might allow a trusted third party (in this case, the government) to read encrypted data in emergencies. They concluded that each approach had significant security risks.

Overall, the cryptographers' view was that introducing this new capability into an encryption system made an already complicated process even more complex. This increased complexity made it more likely that there would be an unintentional vulnerability hidden in the encryption protocol that malicious hackers could find, gaining access to the trusted third party's emergency system or otherwise breaking the code. The hackers could then read secret messages for their own purposes – a huge risk.

When the Clipper Chip project died and when the cryptographers' major study came out, the idea of exceptional access for government seemed to die as well. In an environment in which cybersecurity was an increasing priority, and in which encryption was a partial defense against many data breaches and hackers, it seemed unwise to do anything that might weaken cryptographic standards.

Snowden reveals more

While the Clipper Chip effort to use public processes to create weaknesses in cybersecurity had failed, the National Security Agency had, in secret, worked to undermine certain popular encryption algorithms. In addition to direct attempts to break encryption with mathematical methods, an NSA project code-named Bullrun included efforts to influence or control international cryptography standards, and even to collaborate with private companies to ensure the NSA could decode their encryption.

This came to light when former NSA contractor Edward Snowden revealed a massive trove of files about U.S. government spying in 2013 and reignited the debate about what abilities and powers the government should have to read encrypted material.

Once again, a group of the world's leading cryptographers studied the

issue, and in 2015 came to the same conclusion: The risk of backdooring encryption to enable government access was too high. Doing so would weaken overall security too much to make up for any brief improvements in public safety or national security.

The FBI pushes back

Then came the San Bernardino attack. On Dec. 2, 2015, Rizwan Farook and his wife, Tashfeen Malik, opened fire at a social services center in San Bernardino, California. Inspired – but not directed – by foreign terrorist groups, they killed 14 people and wounded 22 more during their violent rampage.

Before the attack, Farook had physically smashed up two personal cellphones, rendering their data unrecoverable. He left untouched his work phone, an iPhone 5c issued by San Bernardino County. Investigators found the phone, but the FBI was unable to examine its data due to Apple's encryption and security mechanisms on the device.

To get around this, the United States government used a law from the earliest days of the republic, the 1789 All Writs Act, to try to compel Apple to write software that would break the encryption and grant the FBI access. Apple refused, saying that doing so would weaken the security of every iPhone on the market, and a court showdown began.

The conflict in a nutshell

The Apple-FBI case nicely encapsulates much of the debate around encryption: a horrible incident that everyone wants investigated, the government's stated need for access to aid the investigation, strong encryption that prevents that access and a company unwilling to risk the broader security of its products by attacking its own software.

And yet, even when the stakes were as high as the government said they were in the San Bernardino case, encryption would remain secure.

Faced with Apple's refusal to comply and criticism from the technology and privacy industries, the FBI found another way. The bureau hired an outside firm that was able to exploit a vulnerability in the iPhone's software and gain access. It wasn't the first time the bureau had done such a thing.

As this all unfolded, and in the face of a wide range of significant opposition, a bill to mandate backdoors was introduced and failed in the United States Congress.

Encryption backdoors remain largely viewed as weakening everyone's protections all the time for the sake of some people's protections on rare occasions. As a result, workarounds like the FBI found are likely to be the most common approach going forward. Indeed, in recent years, law enforcement agencies have greatly expanded their hacking capabilities.

A look to the future

The details matter, though, and how this fledgling field develops remains to be seen. Technologists and lawyers studying the issue have identified several key questions, but not their answers. These include:

- What kinds of vulnerabilities can law enforcement use to gain access, technologically, legally and ethically?
- Should they report those vulnerabilities to the software vendors for fixing, even if it means it is less likely that either police or hackers will be able use the weaknesses in the future?
- What do they need to tell a judge in order to get permission to hack a device?
- Can they hack devices outside of their jurisdiction, and what

happens if they hack computers in other countries?
- Do they need to tell a defendant at trial how they hacked his or her device?

While some details depend on specific certain answers to these legal and technical questions, a lawful hacking approach offers a solution that appears to gain greater favor with experts than encryption backdoors. A group of scholars proposed some ways we should begin thinking about how law enforcement could hack. Agencies are already doing it, so it's time to turn from the now-ended debate about encryption backdoors and engage in this new discussion instead.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation