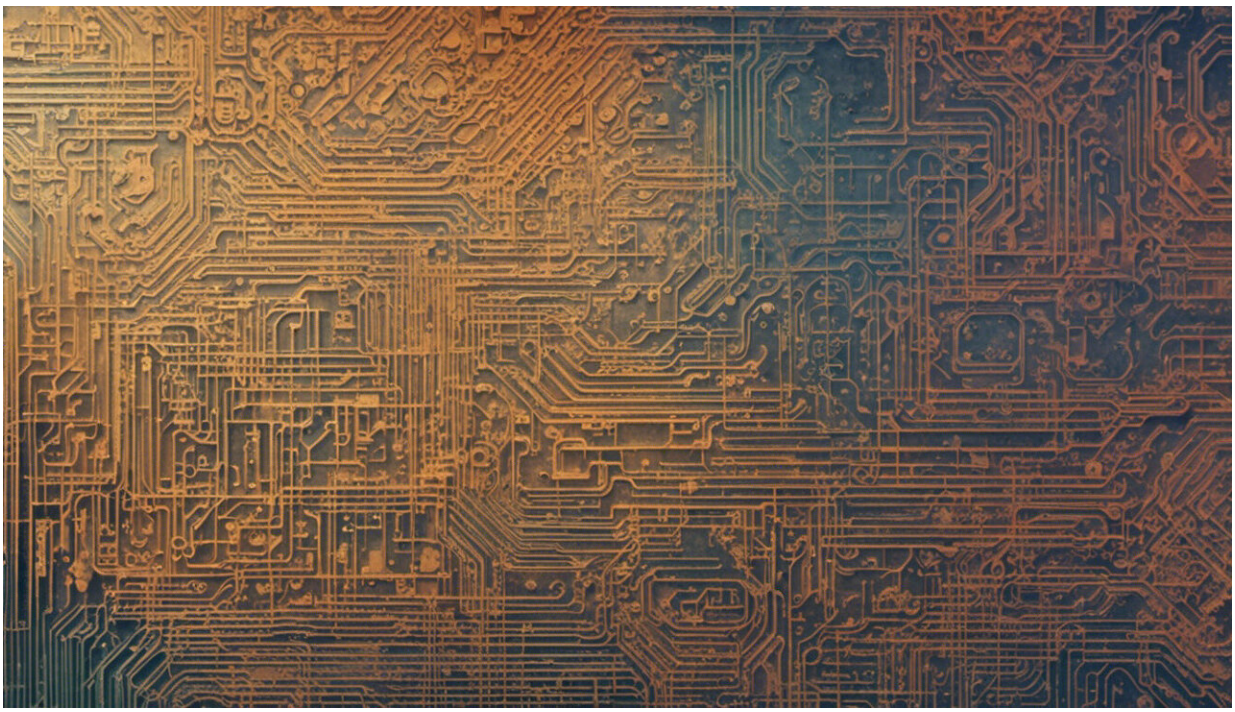
Whether "backdoor" or "front-door," government access imperils your data, experts say

July 9 2015, by Adam Conner-Simons



Credit: AI-generated image (disclaimer)

In recent months, government officials in the United States, the United Kingdom, and other countries have made repeated calls for law-enforcement agencies to be able to access, upon due authorization, encrypted data to help them solve crimes.

Beyond the ethical and political implications of such an approach, though, is a more practical question: If we want to maintain the security of user information, is this sort of access even technically possible?

That was the impetus for a report—titled "Keys under doormats: Mandating insecurity by requiring government access to all data and communications"—published today by security experts from MIT's Computer Science and Artificial Intelligence Lab (CSAIL), alongside other leading researchers from the U.S. and the U.K.

The report argues that such mechanisms "pose far more grave security risks, imperil innovation on which the world's economies depend, and raise more thorny policy issues than we could have imagined when the Internet was in its infancy."

The team warns that rushing to create a legislative proposal is dangerous until security specialists are able to evaluate a comprehensive technical solution that has been carefully analyzed for vulnerabilities.

CSAIL contributors to the report include professors Hal Abelson and Ron Rivest, PhD student Michael Specter, Information Services and Technology network manager Jeff Schiller, and principal research scientist Daniel Weitzner, who spearheaded the work as director of MIT's Cybersecurity and Internet Policy Research Initiative, an interdisciplinary program funded by a $15 million grant from the Hewlett Foundation.

The group also includes cryptography expert Bruce Schneier and researchers from Stanford University, Columbia University, Cambridge University, Johns Hopkins University, Microsoft Research, SRI International, and Worcester Polytechnic Institute.

Not-so-exceptional access

In October, FBI Director James Comey called for what is often described as "exceptional access"—namely, that computer systems should be able to provide access to the plaintext of encrypted information, in transit or stored on a device, at the request of authorized law enforcement agencies.

The research team outlines three reasons why this approach would worsen the already-shaky current state of cybersecurity.

First, it would require preserving private keys that could be compromised not only by law enforcement, but by anyone who is able to hack into them. This represents a 180-degree reversal from state-of-the-art security practices like "forward secrecy," in which decryption keys are deleted immediately after use.

"It would be the equivalent of taking already-read, highly sensitive messages, and, rather than putting them through a shredder, leaving them in the file cabinet of an unlocked office," Weitzner says. "Keeping keys around makes them more susceptible to compromise."

Second, exceptional access would make systems much more complex, introducing new features that require independent testing and are sources of potential vulnerabilities.

"Given that the new mechanisms may have to be used in secret by law enforcement, it would also be difficult, and perhaps illegal, for programmers to even test how these features operate," Weitzner says.

Third, special access in complex systems like smartphones would create vulnerable "single points of failure" that would be particularly attractive targets for hackers, cybercrime groups, and other countries. Any attacker who could break into the system that stores the security credentials would instantly gain access to all of the data, thereby putting potentially

millions of users at risk.

Earlier this spring, the head of the National Security Agency pushed back against assertions that the U.S. government was advocating for a "backdoor," instead suggesting a "front-door" method of unlocking a device using a digital key that is divided into multiple pieces. But researchers argue in the report that such methods "make an attacker's job harder [but] not impossible," and require that mechanisms be decidedly more complex to implement.

Weitzner says that while he recognizes the desire to be able to recover relevant information to solve crimes, he views government eagerness for access as a perilous example of putting the cart before the horse.

"At a time when we are struggling to make the Internet more secure, these proposals would take a step backward by building weakness into our infrastructure," Weitzner says. "It's like leaving your house keys under the doormat: Sure, it may be convenient, but it creates the opportunity for anyone to walk in the door."

More information: "Keys under doormats: Mandating insecurity by requiring government access to all data and communications" dspace.mit.edu/handle/1721.1/97690

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology

access-imperils-experts.html