What the government should’ve learned about backdoors from the Clipper Chip

Sean Gallagher - 12/14/2015, 7:05 PM ⋮ 10-13 minutes ⋮ 12/14/2015

Biz & IT —

The Obama administration's calls for backdoors echo the Clinton-era key escrow fiasco.

The MYK-78 "Clipper" chip, the 1990's version of the "golden key."

In the face of a Federal Bureau of Investigation proposal requesting backdoors into encrypted communications, a noted encryption expert urged Congress not to adopt the requirements due to technical faults in the plan. The shortcomings in question would allow anyone to easily defeat the measure with little technical effort.

Please note, the testimony referenced above was delivered on May 11, 1993. However, that doesn't change its applicability today. In fact, current pressure being applied by law enforcement and intelligence officials over end-to-end encrypted communications appears eerily reminiscent of a similar battle nearly 25 years ago.

Last week, FBI Director James Comey again pushed forward arguments for law enforcement "backdoors" into encrypted communication applications. Comey claimed that the gunmen who attempted to attack a Texas anti-Muslim cartoon event used encrypted communications several times on the day of the attack to contact an overseas individual tied to terrorism. The revelation is part of a renewed lobbying effort to get technology providers to provide what Comey once described as a "golden key" to access encrypted communications. Though the FBI director reluctantly dropped his lobbying efforts for such a backdoor this summer, the attacks in Paris and San Bernardino have raised the issue again. Even President Obama recently asked for technology companies to help give the government access to communications over messaging applications and social media.

The argument *against* backdoors, however, has not changed since 1993. Back then, Whitfield Diffie—one of the creators of the Diffie-Hellman Protocol for secure key exchange—spoke to a congressional hearing about the "Clipper Chip," an encryption chip for digital voice communications announced by the Clinton administration. His main points remain relevant:

- The backdoor would put providers in an awkward position with other governments and international customers, weakening its value.
- Those who want to hide their conversations from the government for nefarious reasons can get around the backdoor easily.
- The only people who would be easy to surveil would be people who didn't care about government surveillance in the first place.
- There was no guarantee someone else might not exploit the backdoor for their own purposes.

Back to the future

The Internet was in its infancy in 1993 when the Clinton administration announced the Clipper Chip. At the time, encryption was being adopted primarily for use on government and private networks, such as the public telephone network and leased data lines. The World Wide Web didn't really exist yet, and commercial Internet providers were only beginning to take off.

Encryption was largely hardware-based at the time because of the limits of computational power. The early '90s standard for encryption in the US was the Data Encryption Standard (DES), developed in the 1970s at IBM on behalf of the

National Bureau of Standards (a forerunner to the modern National Institute of Standards and Technology). DES was already in relatively wide use by the financial industry. And paid satellite services, like HBO and Cinemax, used DES encryption to scramble the audio channels of their transmissions.

But DES, which included some helpful tweaks provided by the National Security Agency, had a problem. If it was built into telephones, it would make it possible for criminals to "go dark" (the same phrasing Comey used to describe the current government concern about encryption). As development of commercial encryption products was starting to grow, the government sought a way to keep that from happening—and it found Clipper.

The Clipper Chip is based on an encryption algorithm called "Skipjack," developed by the NSA in the 1980s. By itself, Skipjack was secure enough to be considered a "Type 1" NSA product, something suitable for government and military use for sensitive communications. Skipjack is ostensibly stronger than DES, based on an 80-bit key while DES' effective keylength was only 56 bits. As of 1993, the algorithm was still classified.

But the extra twist added for the Clipper Chip was key escrow, a feature promoted heavily by then-Vice President Al Gore. The government would keep a record of each tamper-resistant chip's key indexed by its digital signature. Before starting an encrypted session with another chip, Clipper would send a string of data as part of the session initiation called the Law Enforcement Access Field (LEAF)—a hash of an identifying number that would give the government the digital signature needed to get the keys and decrypt the call.

The result was that the government could, in theory, intercept any conversation from any point in the connection—that is, if they could get people to actually use Clipper. "The effect is very much like that of the little keyhole in the back of the combination locks used on the lockers of school children," Diffie told Congress in his 1993 testimony. "The children open the locks with the combinations, which is supposed to keep the other children out, but the teachers can always look in the lockers by using the key."

The government had an added stick: while it could not mandate specific encryption standards, it could offer relaxed export controls on encryption products that used Clipper's key escrow. In the 1990s, encryption tools were subjected to heavy export controls.

The only way to get enough people to use Clipper to make it viable as a tool for the government would have been to ban all other encryption. And as Diffie pointed out, if other encryption was criminal then only criminals would have strong encryption. "It goes without saying that unless unapproved cryptography is outlawed, and probably even if it is, users bent on not having their communications read by the state will implement their own encryption," he told

Congress. And it wouldn't take much to make LEAF ineffective and render Clipper useless as designed—because all they would have to do is add another layer of encryption before Clipper. "Users who have faith in the secret Skipjack algorithm and merely want to protect themselves from compromise via the Law Enforcement Exploitation Field need only encrypt that one item at the start of transmission," he noted.

Despite the concerns of the crypto community, the White House formally rolled out the Clipper Chip in 1994. Luckily, it never achieved the desired acceptance. At the same time, a number of tools based on open encryption standards—including Phil Zimmerman's PGP—became broadly available. Additionally, a number of attacks were developed that rendered the LEAF field useless. Since its key component was a 16-bit hash, it was possible to produce hashes that would be recognized as valid by the Clipper firmware but that would reference the wrong keys.

In 1997, a veritable who's who of the cryptography world at that time—Diffie (then at Sun Microsystems), Bruce Schneier, John Gilmore, MIT's Hal Abelson, Ron Rivest, and Jeffrey Schiller, Ross Anderson, Steven Bellovin and Matt Blaze of AT&T Labs, Microsoft's Josh Benaloh—published a paper excoriating key escrow in general and Clipper specifically. The group asserted, "The deployment of key-recovery-based encryption infrastructures to meet law enforcement's stated specifications will result in substantial sacrifices in security and greatly increased costs to the end user."

Building a secure key management scheme for any key escrow system deployed at a global scale would be too complex and was "far beyond the experience and current competency of the field," the group wrote. "Even if such infrastructures could be built, the risks and costs of such an operating environment may ultimately prove unacceptable. In addition, these infrastructures would generally require extraordinary levels of human trustworthiness."

These problems, they pointed out, were endemic to any key recovery or key escrow approach—"All key-recovery systems require the existence of a highly sensitive and highly-available secret key or collection of keys that must be maintained in a secure manner over an extended time period. These systems must make decryption information quickly accessible to law enforcement agencies without notice to the key owners. These basic requirements make the problem of general key recovery difficult and expensive, and potentially too insecure and too costly for many applications and many users."

The golden key, redux

It's no surprise that the same cryptographers (Diffie et al) have renewed their argument to combat the latest round of calls for a "golden key" to unlock

encrypted communications. Joined by additional authors, in July the group published a new paper that noted the problems facing key recovery systems would be even worse today than they were in the 1990s.

"The complexity of today's Internet environment, with millions of apps and globally connected services, means that new law enforcement requirements are likely to introduce unanticipated, hard to detect security flaws," the group noted. "Beyond these and other technical vulnerabilities, the prospect of globally deployed exceptional access systems raises difficult problems about how such an environment would be governed and how to ensure that such systems would respect human rights and the rule of law."

In August at a question-and-answer session attended by Ars, Comey said he believed the technologists just hadn't tried hard enough to find a way to give government access to encrypted systems. And after the backdoor campaign picked up steam again after the San Bernardino killings, Comey essentially blamed technology companies' "business model" as the reason they didn’t want to provide backdoors.

The renewed talk from the administration has fueled an Electronic Frontier Foundation-led petition campaign calling for President Obama to publicly support strong encryption once and for all. That petition drew a response from US Deputy Chief Technology Officer Ed Felten and Michael Daniel, the president's cybersecurity coordinator. The duo announced the White House would meet with the EFF and others about cryptography policy.

Hopefully, that conversation at the White House will be informed by the lessons of the Clipper Chip.

Previous Chapter Next Chapter