Government Backdoors in Encryption

Abstract

The year was 1993, and for the first time, the National Security Agency of the United States of America released their very own computer chip called the Clipper Chip. This chip was intended to be adopted by telecommunication companies as a secure way to transmit voice data. However, by 1996 it was entirely defunct. Yet the Clipper Chip has a legacy far beyond its use, for it was the US Government's first attempt at adding a backdoor in an encryption algorithm. Since those early days, various governments around the world have dreamt of freely reading their citizens secure communications, even if the information is encrypted. Because electronic communications, both secure and insecure, play such a large part in our lives, the issue of government backdoors has become a huge point of controversy both in the US and abroad. It has become a hot issue not only because backdoors present the technological issue of how to secure a backdoor, but also a moral and ethical issue of citizen's rights to privacy. This debate, though long running, is also coming to a turning point; recent leaks and disclosure have shown that governments and government agencies around the world are trying desperately to intercept as much information as they can, to the point that any non-encrypted communications should simply be considered public. This paper will show that government backdoors in encryption algorithms in any capacity are harmful to end users and should not be allowed.

Introduction

Cryptography is an ancient art, dating back to antiquity when the Romans used a simple cryptographic technique to obscure their messages should their runner be intercepted. But it was not until the digital age that cryptography truly came into its own. The widespread availability and increasing speed of microprocessors led to an immense proliferation of encryption techniques, although they were still overused to securely transmit messages. Although encryption has become much more widespread, the principles behind them have remained mostly unchanged.
Encryption is a way to hide information such that it can only be accessed with a specific key. There are many techniques, but they all hide information by changing the contents of the message in some predictable way. The Romans accomplished this with a technique called a Caesar Cipher, which operates by shifting the characters in the text to be encrypted down the alphabet. For example, the character ‘a’ shifted once is ‘b’, and since ‘z’ is at the end of the alphabet, it becomes ‘a’ when shifted once. In order to decrypt the message once it has been encrypted, one needs only to know the “key” of how much each character has been shifted. This is a very simple encryption method, and the desire to more securely hide information led to the development of the more complex algorithms and techniques which are very commonly used today.

But why do we still encrypt information today? The simple answer is that the internet is very trust-based, and that we have come to rely very heavily on it. Public wifi hotspots, like those found in coffee houses around the world, have proliferated widely, and are often used for sensitive applications like online banking. The problem is that any message you send to your bank on these public networks can be intercepted by anyone else on the network, using a technique called packet sniffing. In order to protect private information from prying eyes, enciphering information has become a highly effective and popular method of establishing privacy.

In fact, encryption has become so effective that governments around the world have taken notice. Many organizations monitor internet traffic to attempt to find evil-doers, from pirates stealing intellectual property to terrorist cells recruiting on internet forums. However, their efforts have been stymied by encrypted communications. This led to the proposal of the Clipper chip, a computer chip to conceal voice transmission from others but leave them open to listening by the NSA. At first glance, the idea of a government backdoor in encryption does not seem like a terrible idea. It would allow government agencies to better detect illegal or dangerous activity on the internet. However, this paper will explain why this is in fact not only a bad idea, but also a dangerous and immoral one.

To the Community
Technology aside, this paper exists as a call to action. American citizens have a fundamental right to privacy; the Bill of Rights states that Americans have the right to “… be secured in their persons, their houses, their papers, and their other property from all unreasonable searches and seizures, shall not be violated by warrants issued without probable cause, supported by oath or affirmation, or not particularly describing the places to be searched, or the persons or things to be seized.” While government agencies searching the internet for hackers may not seem like a violation of civil liberties on its own, the fact that they do so by scanning all internet traffic, searching the traffic of all americans without warrants, makes it a concern. The problem here lies in the fact that the Bill of Rights was written 200 years ago, when the notion of sending messages was limited to paper and word of mouth, and therefore the sixth amendment doesn’t specify electronic communications. However, the intent of the amendment is clear: Americans should be secure in their person, effects, and communications from government search without a warrant. Agencies that monitor internet traffic widely and indiscriminately, especially those trying to institute backdoors in encryption, are violating the basic civil liberty that is privacy.

The world does exist outside of the United States, and government backdoors in encryption has ramifications outside the violation of American civil liberties. For dissidents around the world, the Internet has been a god-send. It has created a way to communicate, share ideas, gain widespread attention, and call out repressive governments when they commit atrocities or punish their people. The Internet has enabled a new wave of openness and dissent largely due to online anonymity, which has been enabled by strong encryption. By using strong encryption, activists can post online, express opinions, and coordinate freely in countries where they may have previously been punished for speaking out. Without this strong encryption, which cannot be broken, this simply would not be possible.

At first glance, government backdoors in the United States may not appear to have bearing on the other side of the planet. However, they are leading the push towards the worldwide adoptions of cryptographic algorithms with a backdoor. Since the United States is a technological leader, this would mean that people around the world would use this fundamentally weak encryption algorithm. This is problematic for a number of reasons. First and foremost, encryption algorithms designed to be accessible to law enforcement must contain some weakness that allows government agencies to break the encryption. In January of 2012, the National Institute of Standards and Technology (NIST) published a set of recommendations
for random number generators. Included in this report was a standard called Dual_EC_DRBG, an algorithm proposed by the NSA, designed to take advantage of the computational complexity of discrete logarithm problem. Theoretically, this could be an incredibly secure random number generator. However, the NIST discovered some oddities in the algorithm that would make it relatively simple for encrypted messages to be decrypted, even without the original key. This insecure method of random number generation could be leveraged by the NSA to decrypt messages, but it also introduced a weakness to any encryption scheme that uses this algorithm.

In this hands of the NSA, knowledge of this weakness is a violation of civil liberties, but should this weakness become know to oppressive regimes, it could be used to crack down on dissent and stifle the flow of information about their actions. This simply cannot be allowed to happen. The United States intelligence services have a storied past with dictatorships from toppling democracies in Latin America in the 1960s, to US involvement in the middle east. Allowing government agencies like the NSA to insert backdoors into encryption algorithms is very dangerous to those in oppressive countries.

**Action Items**

At the bottom of this paper you will find two very important tools. The first is a petition which gained more than 100,000 signatures on the White House website. It is a nation independent petition urging your government to cease and desist attempting to spy on private communications or put backdoors in encryption schemes.

The second tool is list of ways for American readers to contact their elected officials.

I hope that over the course of this paper I have introduced you to the what encryption is, why it is important, and why it should be defended from government tampering. I hope that you have come to understand the dire consequences of government mandated backdoors in encryption algorithms and why they cannot be allowed to exist. I hope that you will use the tools provided below to contact your congressional representatives and tell them that you will not stand for a violation of your civil liberties, and that free and secure encryption helps the entire world be more free and open. Thank you.
Publicly affirm your support for strong encryption.
Reject any law, policy, or mandate that would undermine our security.
The government should not erode the security of our devices or applications, pressure companies to keep and allow government access to our data, mandate implementation of vulnerabilities or backdoors into products, or have disproportionate access to the keys to private data.

We demand privacy, security, and integrity for our communications and systems. As a public, we should be confident that the services we use haven't been weakened or compromised by government mandate or pressure. No legislation, executive order, or private agreement with the government should undermine our rights.
Weakening encryption weakens the entire Internet. Please endorse strong encryption, and encourage other world leaders to do the same.

Find and Contact your Senator:

https://www.opencongress.org/people/zipcodelookup

Contact the White House:

https://www.whitehouse.gov/contact
References


