There should be No Encryption Backdoors, only Front Doors

Robert Thibadeau, Ph.D.
Drive Trust Alliance
www.drivetrust.com
Feb 17, 2016

In two sentences: iPhones and iPads have always had front door central encryption management using international standards. The government needs to learn how to legally employ the solutions that companies have employed for over a decade.

Apple is being taken to the cleaners, unfairly. We agree with their position that a backdoor is dangerous to everybody, particularly the 6 billion people and their families. Everyone needs, and will need, their privacy protected. If you let this genie out of the bottle, it never comes back and you have sacrificed the lives of the many, for the very few.

I recall how, after WWII, maps of France showed streets ending, that that were in fact through streets. The Germans in WWII used the correct French maps to invade. Today, of course, Germany is a world leader in protecting personal and business privacy. Most people have very little idea of what people who want to be malicious can do, even a government. iPhones, iPads and Android devices would have been a huge hole in National Cybersecurity except Apple was first and foremost in protecting user data on iPhones with strong cryptography, and Android is now following suit.

In the mid-2000s, as Chief Technologist for Seagate, I had an exchange with Steve Jobs, who I knew from NeXT days, about the need for hardware encryption on storage devices. Apple took the same position I had already taken at the Trusted Computing Group's Storage Working Group to develop self-encrypting storage devices. There would be no back doors just front doors.

The specifications we developed for industry standard storage device encryption are now part of the experiences of over a billion people a day (see drivetrust.com). Those specifications allow for front doors. Network management of these front doors have been part of the Open Mobile Alliance (OMA) (so called "Mobile Device Management") standards developed years before. I can explain, as I did to Steve before he released his first iPhone.

But let me say that Seagate had already announced self-encrypting drives, and I had already got visits from the law enforcement, and later sat, and still sit, on the American Bar Association's Digital Evidence and eForensics study group. At no time have these guys asked for back doors, although the backdoor concept is often brought up. In fact, once the legal system understands the front door approach, they understand good options they have in doing their jobs.

So, to keep things short, here is the approach: Everybody knows logging in to a PC. In the Trusted Computing Group Storage Specifications and on iPhones and some Android phones you can log into devices to unlock the encryption of user data.

The mechanism to provide a front door is simple and familiar. Nearly everybody today knows about "administrator" or "root" user logins versus “user” logins: Having "administrator" privilege is exactly a front door on user protections. In the storage encryption sphere we have two "administrators." One is the administrator of the storage device itself. The other is the administrator of the users using the encryption. The first administrator sets up the other. This is, quite simply, a front door. The owner of the storage device can control the other administrators and users. This is fundamental to the Trusted Computing Group storage specifications.

Apple is the same. On Apple devices, the device owner is Apple. On our self-encrypting drives the device owner is the first owner of the storage device to set up the login for the device Administrator. So, for example, a company that owns the device can be the device administrator that sets up the encryption administrators and users. We provide for a number of encryption Administrators and a number of Users. Any one Administrator that gets created in effect has alternative access. This is front door access because there are no secrets about it, except for knowing the cryptographic secrets that provides device administrator, encryption administrator, and user access. The Trusted Computing Group standards specify how this can be done, and is done, in an industry standard way for billions of people a day, right now. Mobile device management on iPhones and iPads, and now even Windows 10, does the same.

For law enforcement and digital evidence, the general idea is that local governments can, where appropriate control such access the same way that companies do today. This won’t catch people if their phones are not managed, but it can, and does, catch people based on terms of use. Apple already provides this kind of capability in allowing companies to own specialized applications on the iPhones and iPads from company-private AppStores. The backdoor is in fact the front door.

The Drive Trust Alliance believes that self-encrypting storage hardware, as is on 100% of iPhones and iPads is good. There is a known way to achieve an excellent compromise with privacy and the law and it doesn’t require the device makers to provide backdoors, or really anything new that isn’t already there.

The front doors already exist. Most everybody who uses a PC is already familiar with how the front door approach works. They know about users and administrators. It can work in practice for the good of the people if governments pay attention and develop their procedures around what they already know. A much more vital and useful discussion can be around how to actually employ what we already have technically in place to resolve the dilemma between the good of the many and the good of the few.