COMPUTER AND TECHNOLOGY SECTION

Circuits

Newsletter of the Computer & Technology Section
of the State Bar of Texas

Volume 1: Summer 2014

TABLE OF CONTENTS

Click on the below title to jump to page

What Happened to TrueCrypt?

By Ron Chichester

TrueCrypt was (and still is) a much-beloved open source encryption application. The application has won several awards and was considered by many security professionals to be a first-rate security application. It had entered its seventh major version and was regarded as a mature program. Indeed, it was (and still is) undergoing a major security audit and the initial reports identified only minor problems.

Then, suddenly, in May of this year the original website on truecrypt.org was redirected to a page on SourceForge. The SourceForge page had some rather shocking text, notably "WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues" and "[t]he development of TrueCrypt was ended on 5/2014...". The SourceForge page provided instructions for migrating TrueCrypt-encrypted partitions to Microsoft's Bitlocker – even though partition encryption was but one of the capabilities of TrueCrypt and ignoring its other main use, namely encrypted *containers*.

The SourceForge page provided no reason for this action. Was the TrueCrypt page hijacked by some miscreant? If there was a particular vulnerability, why couldn't it have been fixed and a new version released in the normal course of business just like any other software application? What was the vulnerability? How can you say that TrueCrypt was vulnerable when you don't even know *why* it was vulnerable? Was there a work-around available (which happens often in these types of situations)? Were the developers just sick of the project and wanted out? Why couldn't they just tell us? Their behavior was seemingly aberrant and led to much speculation on Internet websites, blogs and chat rooms.

Some of the speculation centered around the National Security Agency ("NSA"). Such speculation was fueled, in part, because some of the NSA documents disclosed by Edward Snowden mentioned TrueCrypt expressly. The fear was that the NSA was forcing the TrueCrypt developers to compromise their application by installing a "back door" into the source code that would enable the NSA to easily decrypt TrueCrypt containers and disk partitions. This speculation was fueled by none other than Cory Doctorow on the BoingBoing.net blog when he repeated an observation that a cryptic sentence in the SourceForge page (specifically: "Using TrueCrypt is not secure as it may contain unfixed security issues") which when reduced to their

respective first letters can be an anagram for the Latin phrase “uti nsa im cu si” which translates roughly (via Google Translate) to “If I wish to use the NSA”. Would the developers have used something so crass as Google Translate? What are the odds that any of them knew Latin well enough to critique Google Translate adequately? The speculation is that the TrueCrypt developers were pressured by the NSA to compromise the application and the aberrant SourceForge page was a way for those developers to immolate the project rather than allow the NSA to impose a compromise, but in a way that was plausibly deniable that they were doing so because of the NSA.

Who knows? We don't. The developers know (presumably), but they aren't talking. It has been about two months since the switchover of the website. That's long enough for the developers to have gained control of the website from a miscreant. It is also long enough for the developers to provide some insight. Unfortunately, no more information has been forthcoming. The goodwill of the project is being fatally squandered. However, in June it was announced that a fork of the project was being hosted in Switzerland presumably, perhaps foolishly, thinking that the NSA can't reach there. For those who like the program, this is great news, and a testament to the durability of open source software. For others, however, there may just be too many questions and concerns. For them, there are alternatives. The simplest alternative may be 7-zip, which enables 256-bit AES encryption upon compression of the file(s).

About the Author

Ron Chichester practices in the Houston area and specializes in technology-related law, particularly intellectual property, electronic discovery, cybercrimes/cybertorts, electronic commerce and technology licensing. He is a past chair of the Computer & Technology Section of the Texas Bar, and is currently the Chair of the Business Law Section. He is also an Adjunct Professor at the University of Houston where he teaches classes on Digital Transactions (an intellectual property/e-commerce survey course) and Computer Crime. Ron holds a B.S. and an M.S. (both in aerospace engineering) from the University of Michigan and a J.D. from the University of Houston Law Center.