Tap Dancing Around the Fourth Amendment: Encryption for the Internet and for Telephony

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Professor Ric Steinberger, CISSP is one of the most frequent and highly respected instructors in the Norwich University Master of Science program in Information Assurance (MSIA).<http://infoassurance.norwich.edu>. He is also one of my favorite colleagues, with wide interests and a keen eye for interesting articles. He often shares his comments and insights and recently sent such an interesting spontaneous essay about current developments in encryption policy that I asked him to expand it for this column. Everything that follows is entirely his own work with minor edits.

* * *

“It's personal. It's private. And it's no one's business but yours. You may be planning a political campaign, discussing your taxes, or having a secret romance…. Whatever it is, you don't want your private electronic mail… [e-mail] or confidential documents read by anyone else.” These words were first written by Phil Zimmerman<http://bit.ly/6ENqgL> almost 20 years ago (1991, revised in 1999). <http://bit.ly/6ENqgL>

In 1991, Zimmerman released Pretty Good Privacy (PGP)<http://www.mekabay.com/overviews/using_pgp.ppt> and made it available, including source code, by FTP, thus allowing virtually anyone with an Internet connection to download it. At that time, PGP (based on the RSA<http://www.mekabay.com/overviews/using_pgp.ppt> algorithm) was the first freely available public-key based encryption program<http://www.mekabay.com/overviews/using_pgp.ppt>. The net result was that the Internet and e-mail using public had a relatively easy means to use strong encryption to exchange messages that the US government could not read. Strong encryption was (and is) encryption that is essentially unbreakable by large governments employing professional cryptographers who have the world’s most powerful supercomputers at their disposal.

The US government was not amused by PGP, to put it mildly. Zimmerman was accused of violating the Arms Export Control Act and its resultant US International Traffic in Arms Regulations (ITAR) because advanced cryptographic software was considered a munition. Open source cryptography supporters sometimes wore Tee shirts that sported a perl-based implementation of the RSA algorithm followed by the words, “This shirt is a munition”. [Mich Kabay wrote an inflammatory article in Network World in 1993 lambasting the ITAR.<http://www.mekabay.com/infosecmgmt/itar_1993.pdf>] A three year investigation of Zimmerman followed and the government finally dropped its case in 1996.

Flash forward to our own time, and the same kinds of battles are being refought by the US and a number of foreign governments (e.g., India<http://nyti.ms/afwbuR>, UAE<http://nyti.ms/bKxDGn>, and Saudi Arabia<http://nyti.ms/9ZYSR1>). Now, it’s not just e-mail that’s being targeted. It’s commercial mobile telephone networks (especially Blackberry, where the current design does not allow even RIM<http://nyti.ms/bKxDGn>, the company that has developed Blackberry, to decrypt its users’ voice communications). Also under government investigation is virtually every form of Internet-based communication, be it for business or personal use. Examples of applications and protocols now being examined by governments include VoIP<http://nyti.ms/bKxDGn>.
Writer of the New York Times reported on September 27, 2010, “Essentially, officials want Congress to require all services that enable communications … to be technically capable of complying if served with a wiretap order. The mandate would include being able to intercept and unscramble encrypted messages.” <http://nyti.ms/9ZYSRl>

While most people would agree that democratic governments have a right to detect and disrupt individuals engaged in dangerous conspiracies and to intercept and decrypt such groups’ communications, there remain some serious problems with the above approach. The fundamental issue is that the government appears to believe that Internet and wireless digital communications are essentially just modern versions of a 1950s analog telephone call. And we all know that the FBI and police departments have been able to wiretap phone calls for almost as long as there have been telephones.

Right now, governments may be able to browbeat or legally require large telephone companies to implement technical controls that allow for the interception, and if necessary, decryption, of mobile phone calls. It has been alleged, but not proven, that the National Security Agency (NSA), during the Bush administration, pressured several large US telephone companies to provide a means of tapping any phone call that traversed their networks.

It’s not clear today whether RIM, which operates the Blackberry network, would alter its architecture (and possibly its phones) to allow some governments to tap the encrypted conversations and data streams of its customers. Nor is it clear how businesses would react to what could be construed as a serious attack on their security: if governments can tap, then possibly so could some unauthorized third parties.

Furthermore, it’s virtually impossible, given the variety of existing peer-to-peer digital communication applications that support encryption, for any government to decrypt confidential user communications. There’s too much open-source encryption software freely available to everyone to hope to stop encryption altogether.

It’s even more challenging for governments: What about encrypted clouds, possibly hosted offshore? What about photographs or videos of encrypted text posted on photo sharing Web sites or YouTube? What about Steganography, where encrypted materials are embedded in the data stream of pictures or music? What about personal virtual private networks (VPNs)?

For better or for worse, we have irreversibly entered a new age. Governments are going to have to get used to viewing confidential communications either before they are encrypted or after they get decrypted – and with the legal cover of a warrant.

* * *

Ric Steinberger, CISSP, is… (put in a nice juicy biographical paragraph with links and, if you wish, an e-mail address for reader comments).

M. E. Kabay, PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc. and Associate Professor of Information Assurance.

Copyright © 2010 Ric Steinberger & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.