Tap Dancing Around the Fourth Amendment:
Governments Pressuring Encryption Applications

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

In the first of this pair of columns, Prof Ric Steinberger, CISSP of the Norwich University Master of Science program in Information Assurance (MSIA)<http://infoassurance.norwich.edu> reviewed arguments about encryption in the USA in the early 1990s. Today he looks at current pressures around the world being applied to encryption applications.

* * *

Writer Charlie Savage 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/9ZYSRI>

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)<http://www.nsa.gov/>, 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 (e.g., OpenSSL<http://www.openssl.org>, OpenSSH<http://www.openssh.com>, and OpenPGP<http://www.openpgp.org>) freely available to everyone to hope to stop encryption altogether.

It’s even more challenging for governments: What about encrypted clouds<http://www.cloudsecurityalliance.org/>, 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?<http://bit.ly/2Iwe6b> 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< mailto:ricsteinberger@gmail.com >, is a network security consultant
and an adjunct faculty member in Norwich University’s MSIA program. He is also helping
manage a company focused on iPhone applications.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and
operations management consulting services and teaching. He is Chief Technical Officer of
Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor
of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html >
in the School of Business and Management< http://norwich.edu/academics/business/faculty.html
> at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and

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.