Encryption for the Internet and for Telephony: Zimmermann & ITAR Redux

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/cPhMe7> almost 20 years ago (1991, revised in 1999). < http://bit.ly/6ENqgL >

In 1991, Zimmerman released Pretty Good Privacy (PGP) < http://bit.ly/18985Z > 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://bit.ly/A2RI8 > 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 >,< http://nyti.ms/bKxDGn >, and US, < http://nyti.ms/9ZYSRl >, Gulf States http://bit.ly/bwWp6w). 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://www.rim.com/ >, 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://bit.ly/zoAbl > (e.g., Skype, Google Voice) and peer-to-peer chat environments< URL <- Do we really need a URL to explain peer-to-peer to Network World readers? > (e.g., AIM, Yahoo! Messenger, IRC, Windows Live Messenger, and Facebook).

In the next column in this two-part commentary, Prof Steinberger discusses the current controversies brewing around the world over encryption of Internet and mobile telephony communications.

* * *

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 course materials.< http://www.mekabay.com/ >