International Bulletin of Political Psychology

Volume 4 | Issue 15 Article 4

4-16-1998

Trends. An Encryption Paradox: Cracking the Groupe Speciale Mobile Standard (GSM)

Editor

International Bulletin of Political Psychology

Title: Trends. An Encryption Paradox: Cracking the Groupe Speciale Mobile Standard (GSM)
Author: Editor
Volume: 4
Issue: 15
Date: 1998-04-17
Keywords: Encryption, Internet, National Security, Security, Spying, Telecommunications

According to The New York Times, researchers from the University of California at Berkeley's Internet Security Applications, Authentication, and Cryptography Group--along with the director of the Smartcard Developers Association, a computer programmers' organization-- have successfully cracked a widely used encryption method that was designed to prevent the cloning of digital telephones. What may be of even more significance are suspicions that the United States' (US) National Security Agency, Central Intelligence Agency, or other "government spy agencies" may have persuaded encryption designers to mathematically weaken communications security systems and/or to install secret "backdoors"--perhaps even posing as private cryptographers and designing and releasing their own (weakened) encryption programs for commercial use. These suspicions may stem from (1) the alleged finding that the last ten digits of the GSM standard's encryption algorithm key were zeros--a functional shortening of the 64-bit encryption system--(2) long-term US Government (USG) efforts to effect constraints and vulnerabilities concerning encryption methods in the service of national security and the criminal justice system, and/or (3) from various base rates of paranoia that characterize political perceptions and dynamics throughout the world.

Regardless of the truth of the matter, a narrative analysis of US efforts to effect encryption constraints and vulnerabilities in the service of national security and criminal justice suggests the following paradox. Constraints and vulnerabilities become targets for exploitation on the part of security and criminal threats and can lead to legitimate users of encryption being less able to protect themselves. This is evermore the case when the constraints and vulnerabilities are effected less than worldwide--in fact, often unilaterally. As well, the salient meaning of a message or the message itself that is sought by counter-encryptors may be as plain as day but unrecognized respectively as meaning or message. It seems that being hoisted on one's petard is alive and well in an era of globalization and breathtaking telecommunications change. (See Encrypting encryption: Some comments on S.909, Secure Public Networks Act. (August 22, 1997). IBPP, 3(4); Markoff, J. (April 14, 1998). Researchers crack code in cell phones. The New York Times, http://www.nytimes.com; Speech by Louis J. Freeh, Director of the Federal Bureau of Investigation, International Computer Crime Conference, March 4, 1997.) (Keywords: Encryption, Internet, National Security, Security, Spying, Telecommunications.)