IEEE Position Statement

In Support of Strong Encryption

Adopted by the
IEEE Board of Directors

24 June 2018

IEEE supports the use of unfettered strong encryption[1] to protect confidentiality and integrity of data and communications. We oppose efforts by governments to restrict the use of strong encryption and/or to mandate exceptional access mechanisms such as "backdoors" or "key escrow schemes" in order to facilitate government access to encrypted data.[2] Governments have legitimate law enforcement and national security interests. IEEE believes that mandating the intentional creation of backdoors or escrow schemes — no matter how well intentioned — does not serve those interests well and will lead to the creation of vulnerabilities that would result in unforeseen effects as well as some predictable negative consequences.

1. Strong encryption is essential for the protection of individuals, businesses and governments from malicious cyber activities. Encryption protects confidentiality and integrity of data and communications. Almost all of internet commerce relies on encryption to protect data.

2. Exceptional access mechanisms would create risks by allowing malicious actors to exploit weakened systems or embedded vulnerabilities for nefarious purposes. Knowing that exceptional access mechanisms exist would allow malicious actors to focus on finding and exploiting them.[3] Centralized key escrow schemes would create the risk that an adversary would have an opportunity to compromise

[1] For examples of such encryption, see NIST's Computer Security Resource Center, https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Standards.

[2] "The principle of the backdoor is that another third party could have a mechanism to independently and without the knowledge of the sending or receiving party decrypt the communication. In an attempt to protect privacy and unlawful use of the backdoor the concept of key escrow [was created] where the covert cooperation of independent parties with law enforcement would be required to facilitate the use of the backdoor to decrypt the communication." ENISA's Opinion Paper on Encryption: Strong Encryption Safeguards Our Digital Identity, European Union Agency for Network and Information Security (ENISA), December 2016, p. 7.

[3] ENISA, op. cit.

security of all participants, including those who were not specifically targeted.[4] As a result, the risk of successful cyber-theft, cyber-espionage, cyberattack, and cyberterrorism could increase. The consequences of malicious cyber activities to individuals and society might take many forms — including direct financial losses; identity theft; intellectual property theft and theft of sensitive business information; damage to critical infrastructure[5]; damage to national security; reputational damage; opportunity costs such as lost productivity; and even possibly loss of life when computer systems that support essential functions are disabled. Additionally, by increasing the risk of malicious alterations to data, extraordinary access mechanisms could reduce trust in authenticity of data and might lead to decision-making errors and miscalculations.[6]

3. Exceptional access mechanisms would not preclude malicious actors from taking advantage of strong encryption capabilities either created specifically for them[7] or available in countries that have no requirement for exceptional access mechanisms.[8] Devices and systems with strong cybersecurity and/or known not to have exceptional access mechanisms are and would remain readily accessible to the malicious actors whom law enforcement and intelligence agencies wish to monitor.[9]

4. Efforts to constrain strong encryption or introduce key escrow schemes into consumer products can have long-term negative effects on the privacy, security and civil liberties of the citizens so regulated. Encryption is used worldwide, and not all countries and institutions would honour the policy-based protections that exceptional access mechanisms would require. A purpose that one country might consider lawful and in its national interest could be considered by other countries to be illegal or in conflict with their standards and interests. Thus, issues of jurisdiction may be the greatest impediment to exceptional access mechanisms.[10]

[4] The Chertoff Group, "The Ground Truth About Encryption and the Consequences of Extraordinary Access," 2016, https://www.chertoffgroup.com/files/238024-282765.groundtruth.pdf.

[5] Critical infrastructure can be many industry sectors, such as the sixteen listed by the US Department of Homeland Security and established by US Presidential Policy Directive 21. Refer to https://www.dhs.gov/critical-infrastructure-sectors.

[6] Statement for the Record of the US Director of National Intelligence, World Wide Threat Assessment, February 9, 2016, p. 2.

[7] ENISA, op. cit., p. 7.

[8] B. Schneier, K. Seidel, and S. Vijayakumar, 2016, "A Worldwide Survey of Encryption Products," Berkman Center Research Publication No. 2016-2, http://ssrn.com/abstract=2731160.

[9] ENISA, op. cit.; US Director of National Intelligence, op. cit., p. 6.

[10] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, M. A. Specter, and D. J. Weitzner, 2015, "Keys under doormats," *Communications of the ACM*, Volume 58, Issue 10 (October 2015), 24-26, DOI: https://doi.org/10.1145/2814825.

5. Law enforcement agencies have a range of other investigative tools to ensure access to systems and data, when warranted. Techniques include legal mechanisms for accessing data stored in plaintext on corporate servers, targeted exploits on individual machines, forensic analysis of suspected computers, and compelling suspects to reveal keys or passwords.[11]

6. Exceptional access mechanisms could hinder the ability of regulated companies to innovate and compete in the global market. Required exceptional access mechanisms could open an opportunity for non-regulated market participants to create products and services that may appear to customers in the global market to be more trustworthy than warranted.[12]

IEEE is committed to developing trust in technologies through transparency, technical community building, partnership across regions and nations, as a service to humanity. Measures that reduce the security of information or that facilitate the misuse of secure information systems will inevitably damage that trust, which in turn will impede the ability of the technologies to achieve much broader beneficial societal impacts.

ABOUT IEEE

IEEE is the largest technical professional organization dedicated to advancing technology for the benefit of humanity. Through its highly cited publications, conferences, technology standards, and professional and educational activities, IEEE is the trusted voice in a wide variety of areas ranging from aerospace systems, computers, and telecommunications to biomedical engineering, electric power, and consumer electronics.

[11] O. Kerr, B. Schneier, “Encryption Workarounds,” Georgetown Law Journal, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033.

[12] Chertoff, op. cit.