A WHITE PAPER

Risking It All:

Unlocking the Backdoor to the Nation's Cybersecurity

Prepared by

IEEE-USA

The IEEE-USA Committee on Communications Policy (CCP)

With special assistance from CCP members:

Terry Davis
Jon Peha
Eric Burger
Jean Camp
Dan Lubar

IEEE-USA

IEEE

Prepared by

IEEE-USA

The IEEE-USA Committee on Communications Policy (CCP)

With special assistance from CCP members:

Terry Davis
Jon Peha
Eric Burger
Jean Camp
Dan Lubar

ABOUT

This White Paper was prepared by the **Committee on Communications Policy (CCP)** of **The Institute of Electrical and Electronics Engineers-United States of America (IEEE-USA)**, with special assistance from CCP members *Terry Davis, Jon Peha, Eric Burger, Jean Camp, and Dan Lubar.* It represents the considered judgment of a group of U.S. IEEE members with expertise in the subject field. A roster of committee members is provided at the end of this document.

White Papers are designed to provide balanced information on public policy issues in technology-related areas that may affect the interests of technical professionals. This document does not constitute a formal position statement of the IEEE-USA, and its contents do not necessarily reflect the views of IEEE-USA, IEEE, or other IEEE organizational units. IEEE-USA has issued this whitepaper to enhance knowledge and promote discussion of the issues addressed. IEEE-USA advances the public good, and promotes the careers and public policy interests of more than 205,000 engineers, scientists and allied professionals who are U.S. members of the IEEE.

OVERVIEW

This paper addresses government policies that can influence commercial practices to weaken security in products and services sold on the commercial market. The debate on information surveillance for national security must include consideration of the potential cybersecurity risks and economic implications of the information collection strategies employed. As IEEE-USA, we write to comment on current discussions with respect to weakening standards, or altering commercial products and services for intelligence, or law enforcement. Any policy that seeks to weaken technology sold on the commercial market has many serious downsides, even if it temporarily advances the intelligence and law enforcement missions of facilitating legal and authorized government surveillance.[1]

Specifically, we define and address the risks of installing backdoors[2] in commercial products, introducing malware and spyware into products, and weakening standards. We illustrate that these are practices that harm America's cybersecurity posture and put the resilience of American cyberinfrastructure at risk. We write as a technical society to clarify the potential harm should these strategies be adopted. Whether or not these strategies ever have been used in practice is outside the scope of this paper.

Individual computer users, large corporations and government agencies all depend on security features built into information technology products and services they buy on the commercial market. If the security features of these widely available products and services are weak, everyone is in greater danger. There recently have been allegations that U.S. government agencies (and some private entities) have engaged in a number of activities deliberately intended to weaken mass market, widely used technology. Weakening commercial products and services does have the benefit that it becomes easier for U.S. intelligence agencies to conduct surveillance on targets that use the weakened technology, and more information is available for law enforcement purposes. On the surface, it would appear these motivations would be reasonable. However, such strategies also inevitably make it easier for foreign powers, criminals and terrorists to infiltrate these systems for their own purposes. Moreover, everyone who uses backdoor technologies may be vulnerable, and not just the handful of surveillance targets for U.S. intelligence agencies. It is the opinion of IEEE-USA's Committee on Communications Policy that no entity should act to reduce the security of a product or service sold on the commercial market without first conducting a careful and methodical risk assessment. A complete risk assessment

---

1 Jon M. Peha, "The Dangerous Policy of Weakening Security to Facilitate Surveillance," Comments to the U.S. Director of National Intelligence, Oct. 4, 2013. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2350929

2 A **backdoor** is "an undocumented way of gaining access to a computer system. A backdoor is a potential security risk," as defined by the *NIST Guide to Industrial Control Systems Security*.

"...backdoors do not remain secret and the more widespread a backdoor, the more dangerous its existence."

would consider the interests of the large swath of users of the technology who are not the intended targets of government surveillance.

A methodical risk assessment would give proper weight to the asymmetric nature of cyberthreats, given that technology is equally advanced and ubiquitous in the United States, and the locales of many of our adversaries. Vulnerable products should be corrected, as needed, based on this assessment. The next section briefly describes some of the government policies and technical strategies that might have the undesired side effect of reducing security. The following section discusses why the effect of these practices may be a decrease, not an increase, in security.

HOW A GOVERNMENT MIGHT WEAKEN SECURITY

Government policies can affect greatly the security of commercial products, either positively or negatively. There are a number of methods by which a government might affect security negatively as a means of facilitating legal government surveillance. One inexpensive method is to exploit pre-existing weaknesses that are already present in commercial software, while keeping these weaknesses a secret. Another method is to motivate the designer of a computer or communications system to make those systems easier for government agencies to access. Motivation may come from direct mandate or financial incentives. There are many ways that a designer can facilitate government access once so motivated. For example, the system may be equipped with a "backdoor." The company that creates it — and, presumably, the government agency that requests it — would "know" the backdoor, but not the product's (or service's) purchaser(s). The hope is that the government agency will use this feature when it is given authority to do so, but no one else will. However, creating a backdoor introduces the risk that other parties will find the vulnerability, especially when capable adversaries, who are actively seeking security vulnerabilities, know how to leverage such weaknesses.

History illustrates that secret backdoors do not remain secret and that the more widespread a backdoor, the more dangerous its existence. The 1988 Morris worm,[3] the first widespread Internet attack, used a number of backdoors to infect systems and spread widely. The backdoors in that case were a set of secrets then known only by a small, highly technical community. A single, putatively innocent error resulted in a large-scale attack that disabled many systems. In recent years, Barracuda had a completely undocumented backdoor[4] that allowed high levels of access from the Internet addresses assigned to Barracuda. However, when it was publicized, as almost

3 McGraw, Gary, and Greg Morrisett. "Attacking malicious code." *IEEE software5* (2000): 33-41.

4 Dan Goodin, "Secret Backdoors Found in Firewall, VPN Gear from Baraccuda Networks," *Ars Technica*, Jan. 24, 2013. http://arstechnica.com/security/2013/01/secret-backdoors-found-in-firewall-vpn-gear-from-barracuda-networks

inevitably happens, it became extremely unsafe, and Barracuda's customers rejected it.

One example of how attackers can subvert backdoors placed into systems for benign reasons occurred in the network of the largest commercial cellular operator in Greece.[5] Switches deployed in the system came equipped with built-in wiretapping features, intended only for authorized law enforcement agencies. Some unknown attacker was able to install software, and made use of these embedded wiretapping features to surreptitiously and illegally eavesdrop on calls from many cell phones — including phones belonging to the Prime Minister of Greece, a hundred high-ranking Greek dignitaries, and an employee of the U.S. Embassy in Greece before the security breach finally was discovered. In essence, a backdoor created to fight crime was used to commit crime.

"An indirect way to undermine the security of products and services is to influence national or international standards bodies..."

BROADER USE AND ABUSE OF BACKDOORS

Another way to facilitate surveillance by weakening security is to install malware, which typically performs functions invisibly, regardless of the commands or configurations of the customers, owners, or users of a product. Malware can be used to install backdoors, but it can also be used for much more. One common use is to take over machines to sell their processing and communication capacity. Criminals use malware for this purpose, creating networks or machines controlled by a remote entity. These networks are called "botnets." Another common form of malware is spyware, which exports information to an outside entity without the system owner's knowledge or informed consent. Like backdoors, people other than those who install it can use the malware. And like all other systematic weaknesses, the more broadly this weakness is installed, the more the infrastructure and the innocent are at risk.

A more passive way of creating backdoors is not to disclose vulnerabilities of a system or technology when those vulnerabilities are discovered. A robust black market exists for these vulnerabilities. According to one report, an undisclosed vulnerability in widely used commercial software sells for $160,000, on average, on the black market.[6]

THE ROLE OF STANDARDS IN CYBERSECURITY

An indirect way to undermine the security of products and services is to influence national or international standards bodies since many developers build systems that comply with the resulting standards, even when the standards are voluntary. The core of the Internet is not wires or machines; it is standards. Standards make the

5 V. Prevelakis and D. Spinellis, "The Athens Affair," *IEEE Spectrum*, vol. 44, no. 7, July 2007, pp. 26-33.

6 Warwick Ashford, "Black Market for Security Flaws Reaches New Highs," *Computer Weekly*, July 15, 2013. http://www.computerweekly.com/news/2240188014/Black-market-for-software-security-flaws-reaches-new-highs

"Weakened security can only increase the high cost of defending against cybercrime."

Internet work globally across media types (wired, wireless, satellite, etc.), languages, and nations. Standards are required for hardware and software to communicate with other hardware and software across domestic and global Internet systems.

American standards compete with global standards. America's standards-making leadership is a critical advantage, even as more research and production moves offshore. The United States has a history of improving standards and of being global leaders in cryptographic expertise. Consider DES, the standard that allowed electronic funds transfer, the SWIFT network, and first generation data exchanges in the seventies. When the United States strengthened that standard, the standard became resilient to attacks that had not been published and were not widely known. However, entities within the United States could use the precedent of U.S. leadership to deliberately weaken standards. The impact of weakening a standard may be even greater than weakening a specific product or service because that one standard may be used in so many different products and services.

WEAK SECURITY IS DANGEROUS

Improving the ability of law enforcement and intelligence agencies to conduct electronic surveillance is part of a strategy to limit threats from criminals, foreign powers and terrorists. At the same time, strengthening the cybersecurity of systems that private citizens and corporate entities use and engage also limits threats from criminals, foreign powers, and terrorists.

Weak cybersecurity creates opportunities for sophisticated criminal organizations, hostile nation-states, and well-funded, non-state actors. Well-funded criminal organizations will turn to cybercrime for the same reasons they turn to illegal drugs: money and greed. The costs imposed on the rest of us are substantial. The consequences of malicious cyber activities take many forms — including direct financial losses (e.g., fraudulent use of credit cards); intellectual property theft; theft of sensitive business information; opportunity costs, such as lost productivity when a computer system is taken down; and the damage to a company's reputation when others learn its systems have been breached or are vulnerable to compromise. One recent study estimates these costs range from $24 billion to $120 billion per year in the United States.[7] Not only are individuals and enterprises attacked — but also federal, state and local governments.[8] Weakened security can only increase the high cost of defending against cybercrime.

Of course, some technically sophisticated organizations are challenging the security of American computer and communications systems for reasons other than mere financial gain. Finding and exploiting security vulnerabilities is part of how international

---

7 Center for Strategic and International Studies, *The Economic Impact of CyberCrime and Cyber- Espionage*, July 2013.

8 Roberts, P., *Hackers hit small U.S. town, steal tax payer data and $400,000*, in Sophos **Naked Security**, October 15, 2012, retrieved from http://nakedsecurity.sophos.com/2012/10/15/burlington-hacker/ on November 3, 2013.

espionage is conducted in the 21st century, as is clearly demonstrated by recent revelations about Chinese government activities. In addition to economic advantage, foreign governments that compromise the security of contractors to the U.S. Defense Department may use what they learn to improve their offensive and defensive military capabilities. Moreover, as we saw from cyberattacks in Estonia and Georgia, cyberattacks on civilian systems can be highly disruptive to nations and possibly a force multiplier for military or dissident action. The more foreign powers can learn about security vulnerabilities in critical U.S. systems, the more vulnerable the United States is. Worse yet, such malicious behavior is no longer just the domain of nation states. Terrorist organizations also could launch cyberattacks against critical systems. Weakened security only can increase the risk of cyber-espionage, cyberattack, and cyberterrorism.

"The United States might have compromised both security and privacy in a failed attempt to improve security."

If weakened security in commercial products and services is the result of a national policy (as opposed to other causes, such as human error or corporate interests) and that national policy is known or suspected, the weakened security does additional harm to the nation. Similarly, weakened security in support of consumer advertising has the potential to jeopardize the viability of a company's product. Customers naturally will prefer products and services from companies that they believe are immune from such policies and implements. Such U.S. policies could realize a significant negative impact on U.S. competitiveness in the information technology sector. For example, Forrester Research Inc. estimates that recent allegations about U.S. activities may reduce U.S. technology sales overseas by as much as $180 billion, or 25 percent of information technology services, by 2016.[9] As the U.S. information technology sector accounts for a significant portion of the U.S. economy and many high-paying jobs, we suggest such policies are counter to U.S. economic interests in the Information Age.

CONCLUSIONS

The United States benefited greatly from its role as a trusted provider of information and communications technology across the globe. This role cannot be taken for granted. Intelligence and law enforcement agencies that are considering methods of weakening the security of commercial products and services must consider the full range of implications. Similarly, companies that benefit from user data as part of their marketing revenue strategies should consider how their tactics could be abused. Weakened security in standards and mass-market technology can facilitate the authorized surveillance of criminals and terrorists. However, these weaknesses also introduce risk to innocent people, organizations and government agencies, as they become more vulnerable to attack from organized crime, terrorists and foreign powers. If policies to weaken products from the United States are discovered, or

9 Allan Holmes, "NSA Spying Seen Risking Billions in U.S. Technology Sales," *Bloomberg*, Sept. 10, 2013. http://www.bloomberg.com/news/2013-09-10/nsa-spying-seen-risking-billions-in-u-s-technology-sales.html

even merely suspected, U.S. products and services will suffer significant losses — in reputation and business — where trust is critical.

Both supporters and critics of policies to introduce backdoors have presupposed that the alleged activities have reduced privacy to improve security. With that premise, they then argue about whether the nation wins or loses from such a trade. While the debate over how we should value both privacy and security is important, it misses a critical point: *The United States might have compromised **both** security and privacy in a failed attempt to improve security.* A thorough, technically informed, and documented process of risk assessment — with balanced stakeholders from all sides — is needed to ensure the resilience and security of America's cyberinfrastructure, including the Internet and cyberphysical systems.

2014 IEEE-USA CCP MEMBERSHIP ROSTER

2014 OFFICERS:

Terry Davis, Chair
Dan Lubar, Vice Chair
Thomas Tierney, 2014 Vice President, Government Relations
Russell T. Harrison, IEEE-USA Director of Government Relations
IEEE Society Representatives to CCP:
Jean Camp, Society on the Social Implications of Technology (2007)
Goutam Chattopadhyay, Antennas & Propagation Society (2014)
Michael Condry, Industrial Electronics Society (2013)
Upkar Dhaliwal, Region 6 (2013)
Madeleine Glick, Photonics Society (2011)
Weibo Gong, Control Systems Society (2013)
James Isaak, Society for the Social Implications of Technology (2014)
Ferdo Ivanek, Microwave Theory & Techniques Society (2002)
David Kunkee, Geoscience & Remote Sensing Society (2011)
Wayne C. Luplow, Consumer Electronics Society (2014)
Luke Maki, Technology Management Council (2014)
William Meintel, Broadcast Technology Society (2012)
Dhawal Moghe, IEEE Region 5 (2009)
John Newbury, Power & Energy Society (2008)
Tirumale Ramesh, IEEE Region 2 (2006)
Christopher Stiller, Intelligent Transportation Systems Society (2012)
Erdem Topsakal, Engineering in Medicine & Biology Society (2011)
S. Merrill Weiss, Broadcast Technology Society (2012)
Thomas Weldon, IEEE Region 3 (2014)
Gary Yen, Computational Intelligence Society (2010)

MEMBERS:

Brett Berlin
Eric Burger
Jack Cole
William Hayes
Richard Lamb
Stuart Lipoff
Kenneth Lutz
Michael Marcus, Past CCP Chair
Michael Nelson
Jon Peha
Robert Powers
John Richardson
Paul Rinaldo
Bernard Sander
Curtis Siller
Emily Sopensky
Carl Stevenson
Doug Taggart

CORRESPONDING MEMBERS:

Marc Apter, 2013 IEEE-USA President
Gary Belvin
Craig Chatterton
Gerard Christman
Jason Christopher
Sandra Cirlincione
Deborah Cooper
Thomas Cylkowski
Michael McFayden Delaney, Jr.
Hillary Elmore
Matthew Ezovski
Rich Fruchterman
Brett Glass
Keith Grzelak
Nicholas Laneman
Norman Lerner
Scott Lis
David Maxson
Patrick McGlynn
Philip Tomi Olamigoke
Anna Romaniuk
Scott James Shackelford
Glenn Tenney
Norman Turner
Sheree Wen
Philip Wennblom

IEEE-USA
2001 L Street, N.W., Suite 700
Washington, D.C. 20036
T: (202) 785-0017
F: (202) 785-0835
www.ieeeusa.org