The Dangerous Policy of Weakening Security to Facilitate Surveillance

Jon M. Peha

Carnegie Mellon University

peha@cmu.edu

www.ece.cmu.edu/~peha/bio.html

Overview

The American people have an acute and growing need for better cybersecurity protection from numerous threats ranging from identity theft to industrial espionage. The American people also need government law enforcement and intelligence agencies that can conduct effective surveillance against individuals who are involved with crimes or terrorism. Most of the time, these two needs are entirely compatible, but there are occasionally issues on which a balance must be struck. If the balance is wrong, a well-intentioned government agency can severely undermine security rather than strengthen it, and endanger the very American citizens that the agency hopes to protect. Based on recent press reports regarding the alleged activities of the National Security Agency (NSA), it is time for a reevaluation of this balance.

Individual computer users, large corporations, and government agencies all depend on the security features built into information technology products and services that they buy on the open market. If the security features of these widely available products and services are weak, everyone is in greater danger. There have recently been allegations that U.S. government agencies have engaged in a number activities deliberately intended to weaken this widely available technology. Weakening commercial products and services does have the benefit that it becomes easier for U.S. intelligence agencies to conduct surveillance on targets who use the weakened technology, and if it is occurring, this is probably the motivation. However, this strategy also inevitably makes it easier for criminals, terrorists, and foreign powers to infiltrate these systems for their own purposes. Moreover, everyone who uses this technology is vulnerable, and not just the handful who may be surveillance targets for U.S. intelligence agencies. No government agency should act to reduce the security of a product or service sold on the open market without first conducting a careful risk assessment.[1] If the recent allegations in the press are correct, and no such risk assessment occurred, the White House should make sure that a thorough review is conducted now, and that policies are changed as needed based on this assessment.

The next section briefly describes some of the government policies and technical strategies that might have the undesired effect of reducing security. The following section discusses why the effect of these practices may be opposite what their proponents probably intend.

[1] Note that the issues raised in this paper are not necessarily applicable to *targeted* surveillance, such as when a law enforcement agency compromises the security of the specific computer system owned by the principal target of a criminal investigation. This paper is intended to address weakened security in products and services sold on the open market.

How Government Might Weaken Security

Government can greatly affect the security of commercial products, either positively or negatively. This section gives examples of both the technical approaches and policy strategies that might be employed.

An obvious avenue is to convince the designer of a computer or communications system to make those systems easier for government agencies to access. Beginning with the technical perspective, there are many ways that a designer can achieve this if he or she is so motivated. For example, the system may be equipped with a “back door,” which is a method of accessing a system that bypasses the usual security protection. This back door would be known to the company that created it, and presumably to a government agency that requested it, but not to the purchaser of the product or service. 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 back door introduces the risk that other parties will find the vulnerability. This strategy is similar to leaving a large window in your home open for your own use, and simply hoping the neighborhood burglar doesn’t notice, except that in this case it is the government and not the homeowner that propped this window open. In the eyes of security professionals, hope is not a “best practice.” Where there are capable adversaries who are actively seeking security vulnerabilities, this approach can obviously end badly. Moreover, the use of back doors is just one way to create vulnerability by design. A designer might instead embed “spyware” into a system, which is software that captures information and makes it available to an outside party, all without the knowledge or informed consent of the system’s owner. Alternatively, rather than storing and transferring data in encrypted form, a designer may leave information unencrypted at limited times, thereby making surveillance easy for those who know when and where to look. All techniques of this kind become dangerous once they are discovered by adversaries.

One example of how attackers can subvert vulnerabilities placed into systems for benign reasons occurred in the network of the largest commercial cellular operator in Greece.[2] Switches deployed in the system came equipped with built-in wiretapping features that were intended for authorized law enforcement agencies. Some unknown attacker was able to install software that 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 was finally discovered. A vulnerability created to fight crime was used to commit crime.

There are many ways a government can motivate designers to adopt technical approaches such as these. Under a few circumstances, agencies can directly assert the legal authority to mandate these technical design changes. Less obviously, as an enormous purchaser, the federal government can sometimes demand the inclusion of features of interest as a procurement requirement, often making these features a de facto standard in products sold to non-government buyers in the process. Procurement requirements can be used to strengthen security, perhaps by demanding encryption algorithms that are even harder to break than those already on the market, or to weaken security,

[2] V. Prevelakis and D. Spinellis, “The Athens Affair,” *IEEE Spectrum*, vol. 44, no. 7, July 2007, pp. 26-33.

perhaps by demanding a back door. Alternatively, the Government could simply pay commercial companies to compromise the security of their products or services using back doors and other techniques (as some allege has happened).

A less direct way to undermine the security of products and services is to influence standards bodies, since many developers build systems that comply with the resulting standards even when the standards are voluntary. A government agency can sponsor the participation of security experts in important standards bodies, and direct these experts to seek ways to introduce vulnerabilities into standards that the government agency knows how to exploit, instead of directing these experts to make the standards as hard as possible for attackers to penetrate. The impact of weakening standards 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. For example, if one can weaken the standard for a general-purpose encryption algorithm (and it has been alleged that this has already occurred), then it is impossible to predict what will become vulnerable. Perhaps this algorithm will be used to protect stock market transactions, or the real-time control of an electric power grid, or the classified designs of a military aircraft, which would then become vulnerable.

Weak Security is Dangerous

Giving law enforcement and intelligence agencies the ability to conduct electronic surveillance is part of a strategy to limit threats from criminals, foreign powers, and terrorists, but so is strengthening the cybersecurity used by all Americans.

Weak cybersecurity creates opportunities for sophisticated criminal organizations. Well-funded criminal organizations will turn to cybsercrime for the same reason they turn to illegal drugs; there is money to be made. This imposes costs on the rest of us. The costs of malicious cyberactivities take many forms, including direct financial losses (e.g. fraudulent use of credit cards), theft of intellectual property, theft of sensitive business information, opportunities costs such as the 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. One recent study says that estimates of these costs range from $24 billion to $120 billion per year in the U.S.[3] Weakened security can only increase the high cost of 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 espionage is conducted in the 21st century, as is clearly demonstrated by recent revelations about the activities of the Chinese government. 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 action. The more foreign powers can learn about security vulnerabilities in critical systems in the U.S., the more

[3] Center for Strategic and International Studies, *The Economic Impact of CyberCrime and Cyber Espionage,* July 2013.

vulnerable we are. Worse yet, this is no longer just the domain of nation states. Terrorist organizations could also launch cyberattacks against critical systems. Perhaps they will time a cyberattack with a bombing to maximize the damage and the panic. Weakened security can only increase the risk of cyberespionage, cyberattack, and cyberterrorism.

If weakened security in commercial products and services is the result of a national policy (as opposed to other causes such as human error), and that national policy is known or suspected, this does additional harm to the nation. Customers will naturally prefer products and services from companies that they are immune from such a policy.   Thus, such a policy in the U.S. could have a significant impact on the competitiveness of all of the U.S. companies in the information technology sector, which combined account for a significant portion of the U.S. economy, and many high-paying jobs.

Conclusions and Recommendations

There are both supporters and critics of the NSA who have presupposed that the NSA's alleged activities have compromised privacy in order to improve security, and then argued 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: we may have actually compromised both privacy and security in a failed attempt to improve security. It is impossible to fairly judge whether this is the case from a few leaked documents. A detailed examination is needed.

If examination reveals that government actions have indeed weakened the security of widely available products and services, and have done more harm than good in the process, then it is not enough to simply reverse course on those cases that have been uncovered. We must instead develop a more comprehensive approach to assessing risks associated with these practices. It is the NSA's mission to conduct surveillance on individuals that are connected to terrorist organizations or foreign powers, but it is not typically the NSA's mission to protect individual Americans from cyberattacks that lead to credit card fraud, to protect companies from cyberattacks that lead to theft of intellectual property, and to protect the competitiveness of U.S. information technology firms in the global marketplace, even though surveillance decisions made by the NSA could affect all of these. A risk assessment that only considers issues that fall within the NSA's normal scope would inevitably lead to practices that weaken security of commercial products and services even when doing so is harmful to American interests. Effective assessments must consider all of these.

About the author

Jon M. Peha is a professor at Carnegie Mellon University with experience in government, industry, and academia. In government, he has served as Chief Technologist of the Federal Communications Commission, Assistant Director of the White House's Office of Science and Technology Policy, and Legislative Fellow in the House Energy and Commerce Committee.   In industry, he has been the Chief Technical Officer of three high-tech companies. Currently, he is a Carnegie Mellon professor in the Dept. of Electrical & Computer Engineering and the Dept. of Engineering & Public Policy, and former Associate Director of the Center for Wireless & Broadband Networks. He holds a Ph.D. in electrical engineering from Stanford. He is a Fellow of the IEEE, a Fellow of the AAAS, and a member of FCBA and SHPE.