Intelligence and Security Committee submission

Author: Andrew Watson

Date: 6th February 2014

About the Author: This submission is being made in a personal capacity, not as a representative of any organisation. The author has over 30 years' experience in the IT industry. After taking a first in Computer Science from Cambridge, from 1992 onwards he was responsible for specifying, procuring, installing and administering the Internet connection for one of the first UK companies to be connected to the Internet. Other relevant experience includes 6 years' industrial research on distributed computer systems with the Advanced Networked Systems Architecture (ANSA) project, and 20 years' work on open standards for IT.

Summary: The Committee frames its call for evidence by presuming that the individual right to privacy and the collective right to security are opposites that must be balanced. This framing is seriously mistaken when considering the Internet, because the collective security it provides and the privacy of its individual users are fundamentally the same thing.

In recent years the Internet has become part of the nation's critical national infrastructure. Anything that compromises the security (and therefore the privacy) of the Internet's underlying communication mechanisms is a threat to the nation's collective security. Internet providers and users have learned over the past year that UK & US intelligence agencies are actively working to undermine the integrity of the Internet. This is apparently being done to allow them to penetrate the secrecy of their adversaries' communications. However, in doing so, they are compromising the security of every user of the Internet, and thus undermining part of this country's essential infrastructure.

---

1. The Internet has now become part of this nation's critical national infrastructure, essential to Government's daily finances. For example, HMRC received 8.48 million 2012/13 self assessment tax returns via the Internet, representing 84.5% of the total[1] - compared to only 23% seven years earlier.[2] During the course of 2013 HMRC has started operating PAYE "in real time"[3], requiring millions of businesses to use the Internet to submit detailed monthly or weekly reports of the

[1] https://www.gov.uk/government/news/hmrc-sees-record-breaking-year-for-tax-returns

[2] http://webarchive.nationalarchives.gov.uk/+/http://www.hmrc.gov.uk/about/online-filing-figs.htm

[3] http://www.hmrc.gov.uk/payerti/getting-started/rti.htm

tax and National Insurance collected from each individual employee.[4] The integrity of this huge volume of data, and therefore the integrity of the Internet, is now crucial to HMRC's operations.

2. Other financial uses of the Internet are even more widespread. The Office for National Statistics estimates that 25 million people in the UK use the Internet to manage their bank accounts[5] - half of the entire adult population. In 2011 the Payments Council estimated that one in four adults in the UK access their bank account via the Internet every day.[6] Once again, it goes without saying that any threat to the privacy and integrity of the Internet communication between bank and customer would be a major threat to the collective financial security of the nation.

3. Against this backdrop of increasing national reliance on the Internet, the companies that provide this essential service have been startled to learn over recent months that intelligence agencies are working to undermine the fundamental integrity and security of Internet communication. They are doing this in two ways; passively, by failing to pass information about potential security vulnerabilities to Internet equipment manufacturers, and actively, by working to weaken and subvert the widely-used standards that underpin the privacy of internet communication.

4. The intelligence agencies' passive undermining of Internet security stems from their purchase of information about "zero-day vulnerabilities" in Internet infrastructure. Zero-day vulnerabilities are security flaws in Internet subsystems which have been discovered by researchers and cyber-attackers, but which have not yet been reported to the subsystems' vendors. Knowledge of these flaws can be exploited to compromise the security of those sub-systems, and therefore of the Internet as a whole. Although the intelligence agencies do not actually create these vulnerabilities, it has become clear that they are spending millions of pounds of public money[7] purchasing knowledge of zero-day vulnerabilities, but not passing this knowledge on to the Internet equipment vendors concerned.[8] It would seem they are hoarding knowledge of zero-day vulnerabilities so that they can use them against their adversaries, but by doing so, they are knowingly leaving these security vulnerabilities in place. If and when these zero-day vulnerabilities are independently discovered by criminal gangs or hostile nation states, they are used to penetrate UK Internet security and defraud British Internet users.

[4] http://www.hmrc.gov.uk/news/relax-small-business.htm

[5] http://www.ons.gov.uk/ons/dcp171778_322713.pdf

[6] http://www.paymentscouncil.org.uk/media_centre/press_releases/-/page/1523/

[7] https://www.muckrock.com/news/archives/2013/sep/17/nsas-contract-vupen-darth-vader-cybersecurity/

[8] http://www.scmagazine.com/nsa-sought-services-of-french-security-firm-zero-day-seller-vupen/article/312266/

5. Although details are murky, it seems that the intelligence agencies are also actively undermining Internet security by subverting the process of creating public Internet security standards. One specific example discovered in the USA is the deliberate, covert weakening of a standard way of generating pseudo-random numbers called the "Dual Elliptic Curve Deterministic Random Bit Generator" (Dual EC DRBG). This algorithm was devised by the US Government National Institute of Standards and Technology (NIST) and promoted as a standard way of generating very long sequences of numbers that appear to be random, but in fact can be reproduced by someone who knows the "seed" used to initialise the DRBG. Such DRBGs are an essential part of the cryptography that (for instance) prevents criminals interfering with the secure Internet connection between a customer and his/her bank, or between an employer submitting payroll information and HMRC. For a DRBG to be used in this way, it must be impossible to predict the sequence of numbers it will produce without knowing the initial "seed". However, it is now known that US intelligence agencies subverted the process of creating the Dual EC DRBG standard, deliberately introducing a weakness that allowed them (and anyone else who independently discovered the weakness) to predict the sequence of numbers that it would produce without knowing the "seed".[9] Any Internet software supplier using this public standard in their security software would unwittingly be introducing a flaw deliberately created by the US intelligence agencies. This would allow anyone who knew the DRBG flaw to undermine the security provided by that software. As with zero-day vulnerabilities, if a deliberately-created vulnerability is independently discovered by criminal gangs or hostile nation states, it can be used to defraud those who depend on the Internet for secure communication of financial information.

6. The security of the Internet is now crucial to the viability of the United Kingdom and its Government. On its own web page GCHQ says "UK citizens today conduct much of their lives over the internet, as do the Government, the Armed Services, Law Enforcement and industry. For the UK to be safe and successful, the cyber connections and infrastructure we use need to be safe and secure."[10] The safety, security and privacy of each cyber connection made over the Internet is inextricably part of the collective security of the whole Internet. There is no "balance" to be struck between them.

[9] http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html

[10] http://www.gchq.gov.uk/Pages/homepage.aspx