If you seek to 'switch off' encryption, you may as well switch off the whole internet

January 15 2015, by Bill Buchanan

We don’t need any more internet off-switches, thanks. Credit: deadhorse, CC BY-NC

Prime Minister David Cameron has stated that the UK government will look at "switching off" some forms of encryption in order to make society safer from terror attacks. This might make a grand statement but it is impossible to implement and extremely technologically naïve.

Encryption is a core part of the internet; it's use is increasing every day – Google's services, including search and email, use encrypted streams, as do Facebook and Twitter and many other widely used sites. Encryption makes it almost impossible for eavesdroppers to read the contents of the traffic. It is the foundation upon which all e-commerce is based.

It's just impossible to ban. There is no way to define a law which constrains the use of encryption. Would it be only when used in certain applications (such as email), or by disallowing certain methods (such as the encryption program PGP)? Would using a Caesar code, a cipher nearly 2,000 years old, be illegal?

Such a move would make the UK – or any country that followed suit – unsafe in which to do business. Free countries wouldn't consider switching off encryption due to the insecurity it introduces for both consumers and businesses.

Much online content accessed in the UK is actually stored and processed outside the country. Someone who suspects that they may be monitored can set up a secure connection to a remote site in the cloud – Amazon's for example – and store and process information there. How would this fall under any new law?

And where would the ban end? Would it include character encoding, such as the Base-64 encoding that allows for email attachments, or the encoding that provides non-Roman character sets for other languages? Encryption is also the basis for cryptographic signing, a digital signature used by all manner of organisations to verify that digital content – software, audio-visual media, financial products – is what it claims to be. It is the basis of trust on the internet.

We have a right to some privacy. Few people would not object to their letters being examined or their phones being tapped – and the rights

enjoyed in the days of traditional communications should be no different when applied to their modern digital equivalents.

We also have a right to protect ourselves. With major losses of data occurring regularly, whether from attacks or due to error, we need to protect ourselves and our data. Encryption of data when stored or communicated is one way of doing so. The tools used by the security services to hack systems and break encryption are largely the same used by criminal hackers – reducing encryption levels will increase our vulnerability to both.

The trouble with cryptography

Law enforcement agencies have had an easy ride with computer systems and the internet – it's relatively easy to pull evidence from the hard drives of suspects, given the lack of security. But the increasing focus on privacy and security has put the pressure on investigators. The battle lines between the right to privacy and the need to investigate crime have been drawn.

The internet was not designed with security in mind, and most of the protocols in use – HTTP, Telnet, FTP, SMTP – are clear-text and insecure. Encrypted versions such as HTTPS, SSH, FTPS and authenticated mail – are replacing them by adding a layer of security through Secure Socket Layers (SSL). While not perfect, this a vast improvement to a system where anyone can intercept a data packet and read (and change) its contents. The natural step forward is to encrypt the data where it is stored at each end, rather than only as it is transmitted – this avoids what's called a man-in-the-middle attack (interception of traffic en route by a third party impersonating the recipient), and the encryption key needed to decode the message only resides with those who have rights to access it.

Keeping defence on its toes

Reading enemy communications provides a considerable advantage, so cryptography has become a key target for defence agencies. Conspiracy theories have blossomed around the presence of backdoors in cryptography software. Defeating encryption otherwise requires finding a flaw in the methods used (such as the Heartbleed bug discovered in OpenSSL) or with the encryption keys (such as weak passwords).

There has been a long history of defence agencies trying to block and control high-grade cryptography. The US government took copies of encryption keys through its Clipper chip, attempted to prevent publication of the RSA public key encryption method, and dragged Phil Zimmerman through the courts after claiming his PGP ("pretty good privacy") encryption software leaving the country was tantamount to illegally exporting weapons.

Hand me your finger

Ultimately username and password combinations alone are too insecure, as computers are now sufficiently powerful to perform brute-force attacks by checking all possible permutations of characters. The introduction of multi-factor authentication improves this by requiring two or more methods such as passwords, access cards, text messages or even fingerprints.

But Virgina Circuit Court judge Steven C. Fucci ruled last year that fingerprints are not protected by the Fifth Amendment ("no person shall be compelled in any criminal case to be a witness against himself"). This means that those using their fingerprints as access keys may have to offer them up to investigators. Unusually, the same does not apply to passwords.

The UK equivalent, the right to silence, also comes with encryption key-related exceptions: failing to hand them over is an offence in itself.

Encryption by default

Both Apple's iOS and Google's Android operating systems for phones and tablets now offer encryption by default, so that data on their devices are protected straight out of the box. Now that we carry so much data with us on our phones, one might reasonably ask why this took so long.

Of course this ratchets up the tension between privacy and police investigation. With iOS 8 and Android Lollipop, there are no electronic methods to access encryption keys from existing digital forensics tool kits, nor will the users have a password to hand over, so the encryption method technically breaches the law in both the US and UK. The same battle rages over the encrypted web service Tor which law enforcement sees as a domain where crime can go undetected, but the privacy-minded advocate see as an important bulwark against authoritarianism.

The technical case for switching off encryption is simply a non-starter. In fact we are moving in the opposite direction, replacing the old, open internet with one that incorporates security by design. If you wish to switch off encryption, it will unpick the stitching that holds the internet together.

Source: The Conversation

internet.html