

Article development led by **acmqueue**
queue.acm.org

Retaining electronic privacy requires more political engagement.

BY POUL-HENNING KAMP

More Encryption Means Less Privacy

WHEN EDWARD SNOWDEN made it known to the world that pretty much all traffic on the Internet was collected and searched by the U.S. National Security Agency (NSA), the U.K. Government Communications Headquarters (GCHQ), and various other countries' secret services as well, the IT and networking communities were furious and felt betrayed.

A wave of activism followed to get traffic encrypted so as to make it impossible for NSA to indiscriminately snoop on the entire world population. When all you have is a hammer, all problems look like nails, and the available hammer was the SSL/TLS encryption protocol, so the battle cry was “SSL/TLS/HTTPS everywhere.” A lot of nails have been hit with that!



After an animated plenary session in Vancouver, the Internet Engineering Task Force (IETF) published “Best Current Practice 188” (<https://tools.ietf.org/html/bcp188>), which declared that pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols where possible. Now, with this manifesto in hand, SSL/TLS and encryption are being hammered into and bolted onto protocols and standards throughout the IETF working groups.

Victory—*privacy*—seemed certain. Or maybe not.

► Kazakhstan recently announced that a “state root certificate” would have to be installed on all computers



wanting to use SSL/TLS/HTTPS out of the country.

► France's ministry of the interior is working on banning free WiFi connections and the use of the Tor protocol and networks.

► President Obama urged high-tech and law enforcement leaders to make it more difficult for terrorists to use technology to escape from justice.

Other countries, notably the U.K., are also working to clamp down on encryption. The Great Firewall of China has been in operation for a number of years, and for all we know, the NSA's total monitoring of the Internet continues unabated 2.5 years after Snowden revealed it to the world. The things worth noting here are:

► Kazakhstan did not just require criminals to install the "state root certificate" so their communications could be scrutinized, it required everybody in Kazakhstan to do so.

► France will not just ban criminals from using free WiFi and Tor, it will ban anybody and everybody from using them.

► While Obama wants to make it "harder for terrorists," I don't think he contemplates Apple offering an "OS X terrorist edition" or that terrorists will take an FBI-sponsored "Are you a terrorist?" quiz to find out if they should be using it.

Whatever the high-tech and law enforcement leaders decide, it will apply to everybody.

How Did More Encryption Cause Less Privacy?

In Terry Pratchett's *Going Postal*, the hero postmaster, Moist von Lipwig, has a knack for noticing what is not in a text. He would have had a field day with BCP188 because none of the following words are anywhere to be found:

- law
- court
- crime
- human
- secret
- warrant
- espionage
- constitution
- jurisdiction

It was not by accident, mind you, the authors of the document deliberately

stayed clear of anything that could even faintly smell of “politics.” Unfortunately, that is not the way politics works. Politics springs into action the moment somebody disagrees with you because of their political point of view, even if you think you do not have a political point of view.

In spite of leaving out all those “hot” words, the substance of BCP188 is still a manifesto declaring a universal human right to absolute privacy in electronic communications—no matter what.

That last bit is half the trouble—no matter what.

Even against law enforcement.

Even if law enforcement has a court order.

Even if ...

No matter what.

To be totally fair, BCP188 nowhere states “no matter what.” The real reason the result ends up being “no matter what” is the SSL/TLS protocol, when properly configured, works as advertised: there is no way to break it.


The other half of the trouble is the hallmark of a civilized society is a judicial system that can right wrongs, and therefore human rights are always footnoted. The United Nation’s Human Rights Charter has §29.2, which explains:

“In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.”


Politicians, whose jobs are to maintain “public order” and improve “the general welfare,” follow the general principle that if criminals can use X to commit crimes, the legal system should be able to use X to solve crimes, with only two universally recognized exemptions: when “X = your brain” and when “X = your spouse.”

For instance, U.S. kids learn in school that the Fourth Amendment affords a right to privacy, but that is only the first half of it. The second half details precisely how and why you may lose that privacy:

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search-



When all you have is a hammer, all problems look like nails, and the available hammer was the SSL/TLS encryption protocol, so the battle cry was “SSL/TLS/HTTPS everywhere.” A lot of nails have been hit with that!




es and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

As this example also shows, wise lawmakers are wary of making it too easy for the legal system, so they add checks and balances.

Political strategies regarding cryptography are all horrible: Kazakhstan brutally inserts state monitors into the middle of all encrypted traffic. France forbids all online anonymity. The U.S. wants backdoors built into all crypto. These ideas are all based on the same principle: If we cannot break the crypto for a specific criminal on demand, we will preemptively break it for everybody. And whatever you may feel about politicians, they do have the legitimacy and power to do so. They have the constitutions, legislative powers, courts of law, and police forces to make this happen.

The IT and networking communities overlooked a wise saying from soldiers and police officers: “Make sure the other side has an easier way out than destroying you.”

But we didn’t, and they are.

Slapping unbreakable crypto onto more and more packets is just going to make matters worse. The only way to retain any amount of electronic privacy is through political engagement. 

Related articles on queue.acm.org

More Encryption Is Not the Solution

Poul-Henning Kamp

<http://queue.acm.org/detail.cfm?id=2508864>

Hickory Dickory Doc

George Neville-Neil

<http://queue.acm.org/detail.cfm?id=2791303>

Compliance Deconstructed

J. C. Cannon and Marilee Byers

<http://queue.acm.org/detail.cfm?id=1160449>

Poul-Henning Kamp (phk@FreeBSD.org) is one of the primary developers of the FreeBSD operating system, which he has worked on from the very beginning. He is widely unknown for his MD5-based password scrambler, which protects the passwords on Cisco routers, Juniper routers, and Linux and BSD systems.

Copyright held by author.
Publication rights licensed to ACM. \$15.00.