More Encryption Is Not the Solution

Cryptography as privacy works only if both ends work at it in good faith

By Poul-Henning Kamp

The recent exposure of the dragnet-style surveillance of Internet traffic has provoked a number of responses that are variations of the general formula, “More encryption is the solution.” This is not the case. In fact, more encryption will probably only make the privacy crisis worse than it already is.

INCONVENIENT FACT #1 ABOUT PRIVACY | **Politics Trumps Cryptography**

Nation-states have police forces with guns. Cryptographers and the IETF (Internet Engineering Task Force) do not.

Several nation-states, most notably the United Kingdom, have enacted laws that allow the police to jail suspects until they reveal the cryptographic keys to unlock their computers. Such laws open a host of due process and civil rights issues that we do not need to dwell on here. For now it is enough to note that such laws can be enacted and enforced.

INCONVENIENT FACT #2 ABOUT PRIVACY | **Not Everybody Has a Right to Privacy**

The privacy of some strata of the population has been restricted. In many nation-states, for example, prisoners are allowed private communication only with their designated lawyers; all other communications must be monitored by a prison guard.

Many employees sign away most of their rights to privacy while “on the clock,” up to and including accepting closed-circuit TV cameras in the company restrooms.

Any person can have the right to privacy removed through whatever passes for judicial oversight in their country of residence, so that authorities can confirm or deny a suspicion of illegal activities. People in a foreign country may not have any right to privacy. Depriving them of their privacy is called “espionage,” a fully legal and usually well-funded part of any nation-state’s self-defense mechanism.

INCONVENIENT FACT #3 ABOUT PRIVACY | **Encryption Will Be Broken, If Need Be**

This follows directly from the first two points: if a nation-state decides that somebody should not have privacy, then it will use whatever means available to prevent that privacy. Traditionally, this meant intercepting mail, tapping phones, sitting in a flowerbed with a pair of binoculars, installing “pingers,” and more recently, attaching GPS devices to cars.

Widely available, practically unbreakable cryptography drastically changed the balance of power, and the 9/11 terrorist attack in New York City 12 years ago acted as a catalyst throughout the world for stronger investigative powers that would allow plans for terrorist activity to be discovered before they could be carried out.

Skype offers an interesting insight into just how far a nation-state is willing to go to get past encryption. Originally, Skype was a peer-to-peer encrypted network, and although the source or

encryption scheme was never made available for inspection, it was assumed to be pretty good. Then something funny happened: eBay bought Skype for a pile of money with some vague explanation about allowing buyers and sellers to communicate directly.

To me, as an experienced eBay user, that explanation didn't make any sense at all, certainly not for the kinds of goods I usually purchase—such as vintage HP instrumentation. I assumed, however, that other user segments—perhaps stamp collectors or garden-gnome aficionados—had different modes of trading.

Then some weird rumors started to circulate: eBay had bought Skype without the source code and regretted the purchase. There seemed to be something to those rumors, because eBay sold Skype back to the founder, for a lot less money.

Head scratching now became a serious risk of baldness for people trying to keep track, because then Microsoft bought Skype for a pile of money, and this time the purchase included the source code. Then Microsoft changed the architecture: it centralized Skype so that all Skype conversations would go through a Microsoft server somewhere in the world. At this point human rights activists who had relied on Skype for a clear channel out of oppressive regimes started to worry.

Some may speculate that the disclosures by former NSA (National Security Agency) contractor Edward Snowden seem to support the theory that Microsoft bought Skype to give the NSA access to the unencrypted conversations through Skype, although we don't know if that's the case, nor what NSA paid for Microsoft's assistance if so.

With expenditures of this scale, there are a whole host of things one could buy to weaken encryption. I would contact providers of popular cloud and “whatever-as-service” providers and make them an offer they couldn't refuse: on all HTTPS connections out of the country, the symmetric key cannot be random; it must come from a dictionary of 100 million random-looking keys that I provide. The key from the other side? Slip that in there somewhere, and I can find it (encrypted in a Set-Cookie header?).

In the long run, nobody is going to notice that the symmetric keys are not random—you would have to scrutinize the key material in many thousands of connections before you would even start to suspect something was wrong. That is the basic problem with cryptography as a means of privacy: *it works only if both ends work at it in good faith.*

Major operating-system vendors could be told to collect the keys to encrypted partitions as part of their “automatic update communication,” and nobody would notice that 30-40 extra random-looking bytes got sent back to the mother ship. That would allow any duly authorized officer of the law simply to ask for the passwords, given the machine's unique identifier. That would be so much more efficient and unobtrusive than jailing the suspect until he or she revealed it. For one thing, the suspects wouldn't even need to know that their data was under scrutiny.

Building backdoors into computing devices goes without saying. Consider the stock-quote application for my smartphone, shown in figure 1. I can neither disable nor delete this app, and it has permission to access everything the phone can do.

No, I don't trust my smartphone with any secrets.

You could also hire a bunch of good programmers, pay them to get deeply involved in open source projects, and have them sneak vulnerabilities into the source code. Here is how the result could look:

In September 2006, somebody pointed out that Valgrind complained about a particular code

FIGURE 1

Stock-Quote Applications

Stock-quote app splash screen

Stock-quote app permissions

More stock-quote app permissions

line and managed to get it removed from the Debian version of OpenSSL. Only two years later did somebody realize that this reduces the initial randomness available to the cryptographic functions to almost nothing: a paltry 32,000 different states.¹

As spymaster, I would have handed out a bonus: weakening cryptographic key selection makes brute-force attacks so much more economical.

Open source projects are built on trust, and these days they are barely conscious of national borders and largely unaffected by any real-world politics, be it trade wars or merely cultural differences. But that doesn't mean that real-world politics are not acutely aware of open source projects and the potential advantage they can give in the secret world of spycraft.

To an intelligence agency, a well-thought-out weakness can easily be worth a cover identity and five years of salary to a top-notch programmer. Anybody who puts in five good years on an open source project can get away with inserting a patch that "on further inspection might not be optimal."

POLITICS, NOT ENCRYPTION, IS THE ANSWER

As long as politics trumps encryption, fighting the battle for privacy with encryption is a losing proposition. In the past quarter century, international trade agreements have been the big thing: free movement of goods across borders and oceans, to the mutual benefit of all parties.

I guess we all assumed that information and privacy rights would receive the same mutual respect as property rights did in these agreements, but we were wrong.

We can all either draw our cloud services back home or deal only with companies subject to the same jurisdiction as us—insist on “Danish data on Danish soil,” and so on. This already seems to be a reflex reaction in many governments—there are even rumors about an uptick in sales of good old-fashioned typewriters. That will solve the problem, but it will also roll back many of the advantages and economic benefits of the Internet.

Another option is to give privacy rights the same protection as property rights in trade agreements, up to and including economic retaliation if a nation-state breaks its end of the bargain and spies on citizens of its partner countries. This is not a great solution (it would be hard to detect and enforce), but it could sort of work.

The only surefire way to gain back our privacy is also the least likely: the citizens of all nation-states must empower politicians who will defund and dismantle the espionage machinery and instead rely on international cooperation to expose and prevent terrorist activity.

It is important to recognize that there will be no one-size-fits-all solution. Different nation-states have vastly different attitudes to privacy: in Denmark, tax forms are secret; in Norway they are public; and it would be hard to find two nation-states separated by less time and space than Denmark and Norway.

There will also always be a role for encryption, for human-rights activists, diplomats, spies, and other “professionals.” But for Mr. and Mrs. Smith, the solution can only come from politics that respect a basic human right to privacy—an encryption arms race will not work.

REFERENCE

1. Schneier, B. 2008. Random number bug in Debian Linux. Schneier on Security blog; http://www.schneier.com/blog/archives/2008/05/random_number_b.html.

LOVE IT, HATE IT? LET US KNOW

feedback@queue.acm.org

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. Some people have noticed that he wrote a memory allocator, a device file system, and a disk-encryption method that is actually usable. Kamp lives in Denmark with his wife, his son, his daughter, about a dozen FreeBSD computers, and one of the world’s most precise NTP (Network Time Protocol) clocks. He makes a living as an independent contractor doing all sorts of stuff with computers and networks.

© 2013 ACM 1542-7730/13/0700 \$10.00