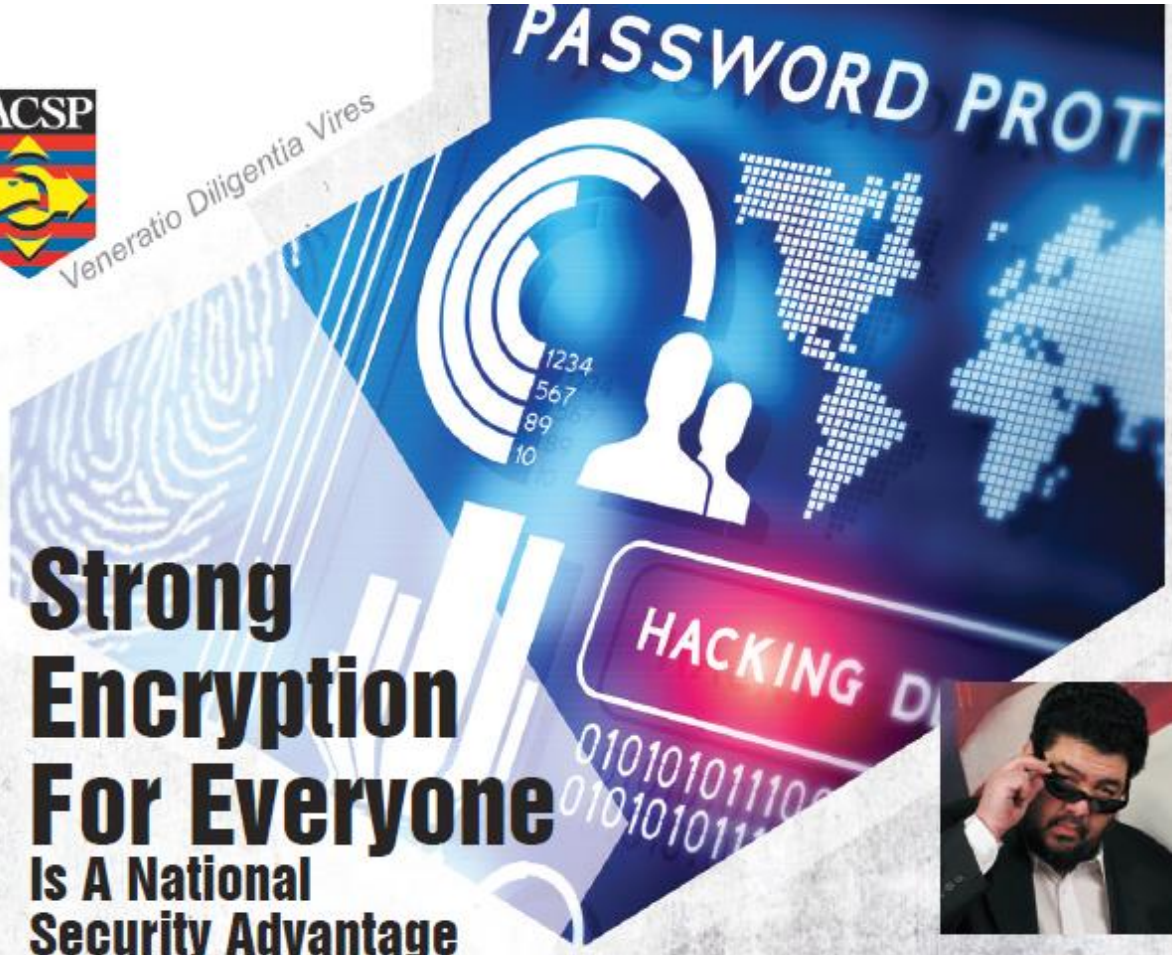

Strong Encryption For Everyone

Is A National Security Advantage

By David Gewirtz

In the wake of recent terrorist attacks, citizens and those responsible for protecting them are asking the same questions. How could the attacks have happened? What else could we have done to prevent them? What should we have known that we didn't know?

Many of those questions eventually lead to the subject of intelligence gathering. If only we knew ahead of time what the terrorists were planning, perhaps we could have stopped them. If only we knew who to suspect, perhaps we could have looked into them -- and then stopped them.

If only we knew ...

If only we could listen in on their conversations, read their e-mail, sift through their social network conversations. If only we could get ahead of the attack, if only we knew what they were saying, then we could have taken action.

Gathering that information is a formidable challenge that ranges from the policy and privacy concerns of citizens to technological issues. In this article, we're going to ignore the very complicated and important privacy and policy issues and go straight to the technical problem: how can we know?

The key premise here is that there is an ongoing stream of data being transferred and if we could somehow tap into that stream, read it all, and take intelligent action based on the incredibly tiny fraction of the data, that's meaningful from a counter-terrorism perspective, we might prevent another attack.

Most of the issues of tapping into the various streams are solvable from a partnership or legal perspective. Agencies work with some private companies -- often as a result of a court order -- to tap into some information flow and derive some targeting value. Again, for the purpose of this article, let's assume that works well enough. Let's again delve further down, into a technical issue: encrypted communication.

Because once we have the policy and judicial approval to tap into digital communication, and once we have the ability to get a data stream from the vendors (or from, uh, "other" sources), if the messages themselves are encrypted, we still have to be able to decrypt them to read them.

Given that it's relatively obvious to terrorists and criminals that law enforcement and national security organizations will be attempting to read their messages, it's not a big jump for them to decide to use strong crypto to protect their communications from prying eyes.

That brings us to our current challenge: bad guys are encrypting their messages and if we could decrypt them, we could read them -- and possibly prevent another attack.

An obvious -- but dangerously incorrect answer -- would be to make sure that government and law enforcement can crack any encryption the bad guys might use, usually through the use of "back door" vulnerabilities built right into the encryption technology.

This is an approach being actively advocated by legislators and national law enforcement officials, particularly when it comes to smartphone-based communications and other consumer-level communications protected by high-quality encryption.

They reason that if there were back doors engineered into the cryptography algorithms, then once authorized by an appropriate oversight body, they could easily flip a switch and listen into any such authorized conversation.

It seems to make sense, but building in back doors is a very, very bad idea. Here are six reasons why:

1. Back doors are deliberately engineered flaws in the system. Any flaw that we can exploit can be found and exploited by our enemies. Since this is an asymmetric battle, if we engineer flaws into things like smartphones, we are -- by design -- subjecting every smartphone user to penetration by the enemy. Back doors are a gift to the enemy.

2. Back doors give the enemy an excuse to innovate. If we

build back doors into our systems, it's not like enemy actors won't know. The fact is, they'll find alternate ways to hide their communications, most likely building their one encryption technology in secret. So not only will we still have to crack encryption, we'll have to find out what it is first.

3. Don't assume terrorists don't have access to top technology skills. As an example, back in 2012, I wrote about Iran's investment in higher education. Despite seeming backwards in some areas, the nation has more than 3.5 million college students, 40,000 masters-level students, and 20,000 Ph.D. students. Back then, more than 20 million Iranians were online. So while I would never recommend you conflate terrorists with Iranians, it's important to realize that Iran is representative of the sort of nation that produces terrorists -- and many of them are technologically astute.

4. Back doors and encryption flaws open the door to other forms of spying. Don't just assume that back doors will be exploited only by governments and terrorists. Back doors will open the door to industrial espionage of an unimaginable level. While allies have always spied on each other, once it's easy to crack encryption, everyone will be doing it -- and no secret or competitive advantage will be safe.

5. Privacy isn't just about people hiding stuff. If bad guys, terrorists, enemy states or others can access personal, private information (like normally-protected health care secrets), the potential for blackmail increases exponentially.

6. Engineered-in back doors will be used by individuals as well. Once engineered-in back doors are created, you can bet those exploits will be for sale online. And then you can bet that scumbags (as distinguished from terrorists and enemy states) will use that information for stalking, harassment, and other run-of-the-mill bad behavior that might otherwise be kept in check.

Perhaps, most importantly, an engineered-in back door gives up our asymmetric advantage. You see, while the terrorists' asymmetric advantage is they can hit any one target and we have to protect them all, our asymmetric advantage is our enormous economic and industrial might (and enormous brain trusts like those at the NSA and in companies like Google and Apple).

If we build encryption that anyone can crack with the right codes, anyone can crack it. But if the very best encryption is out there and used by everyone, the only ones with the resources to possibly crack it -- doing it the hard way -- is us, because we have more resources than anyone else to throw at the problem.

So here are the talking points you should take back to your agencies, departments, and organizations. One, built-in encryption back doors will be used against us more than it will help us. Two, if we build in back doors, the bad guys will engineer alternate encryption solutions. And finally, if we let encryption be the best it can be, we will be the only ones with the resources to crack that encryption - the old fashioned way. By actually breaking the code.

So here are the talking points you should take back to your agencies, departments, and organizations. One, built-in encryption back doors will be used against us more than it will help us. Two, if we build in back doors, the bad guys will engineer alternate encryption solutions. And finally, if we let encryption be the best it can be, we will be the only ones with the resources to crack that encryption -- the old fashioned way. By actually breaking the code.

And it's not like we haven't used our overwhelming code breaking skills before. This is what we do.

About the Author

David Gewirtz is Director of the U.S. Strategic Perspective Institute, Distinguished Lecturer for CBS Interactive, Cyberwarfare Advisor for the International Association of Counterterrorism and Security Professionals, IT Advisor to the Florida Public Health Association and an instructor at the UC Berkeley extension.