HOGE FENTON
Hoge Fenton Jones & Appel
Attorneys at Law | Founded in 1952

Data Protection by Encryption: Use a Random, Nondeterministic Seed

By: Dan Minutillo
Email: dm@hogefenton.com
San Jose: 408.287.9501

Encryption technology and products which use or contain encryption are controlled on export from the United States and further controlled on import by many countries in the world. The import customs regimes of governments such as China, Russia, France, among other countries, are careful about certain types of cryptography crossing the border to enter the country. Other countries like the United States and countries in the European Union control the worldwide movement of products which use or contain encryption using restrictive export regulations as the product moves out of those countries. Cryptography is controlled "coming and going"!

The ulterior motive of Governments around the world, including the United States, to control products which use or contain encryption, is to have a review process in place based on an export or import regime so that enough information can be gathered about the cryptography used in the product to break it (to determine the key) so that a Government could have the opportunity to access, mine, compile, and analyze protected data contained in a computer, on a server, or in the cloud, if that data is needed by that Government for whatever purpose, legitimate or otherwise.

Because of these export and import restrictions and controls on products which use or contain encryption, to ensure compliance with law, companies that create commercial software and hardware products for worldwide use, unfortunately need to be just as interested in key length, substantial support criteria, static and dynamic linking, satisfying mass market or ENC license exception criteria, quantum crypto, or open cryptographic interface issues to qualify for export and import license exceptions in order to sell their product worldwide, as with the functionality and strength of their cryptography.

Business life would be so much easier and less stressful if a hospital, a bank, a law firm, an employer, or a hardware or software manufacturer never had to worry about a breach in its data security system by a hacker. For data protection purposes, commercial companies whose products use or contain encryption should be able to solely focus on providing better security rather than being burdened with export and import compliance requirements in order to avoid having to obtain export or import licenses or authorizations when selling products worldwide.

It is possible to create unbreakable crypto, but the resulting encryption product would be difficult to export from the United States and even more difficult to import into various countries around the world without export and/or import licenses, and without being forced to reveal keys or at least processes used to create keys to some foreign Governments.

This is shortsighted by Governments. Encouraging rather than stifling the creation, export and import of unbreakable encryption provides huge benefits to Governments and to its citizens around the world

because unbreakable encryption protects the homeland from data breach through an intrusive cyber-attack and in turn protects classified and unclassified Government information which could be used to compromise public safety, national security or homeland security.

Allowing unrestricted export and import of unbreakable encryption to US allies strengthens them which in turn strengthens the US. We don't need to know our allies secrets so long as our respective self-interests and motives are aligned. More important, as the US has recently experienced, once it is published that a Government has broken into the private sanctum of foreign political leaders electronic communications, the long term, devastating effect on world-wide reputation, trust, and later, accommodation, usually far outweighs what is gained and actually considered valuable.

The sad reality is that if Governments were more interested in the commercialization and commercial advancement and sale of data protection products for worldwide use, a cost efficient, commercially used, unbreakable encryption key would be close at hand because companies that produce products which use or contain encryption would only need to focus on true data security and not export and import compliance. Unbreakable crypto could be created using a nondeterministic, unpredictable, random, fluctuating "seed."

What is a "seed" in crypto terms? A seed is a key used to initialize a cryptographic device—it allows encryption to work for its intended purpose. From a lay viewpoint, encryption starts when a computer (a program) generates a seed. A seed, for example, could be created from a "moment in time" as measured or stated by a streamed number from a computer's clock or from any numerical stream available. In its simplest form, that moment in time, or part of it, as streamed by the computer can be multiplied, for example, against a second moment in time or against itself and the repetition continues as a key is developed. The computer performs a calculation to create a seemingly random number which is used as a key to lock down data.

Considering the present state of crypto technology, most seeds are deterministic. A fast, powerful computer or virtual network of computers can run calculations to have the seed repeat itself and thereby identify it. Once the seed is determined, breaking crypto to access, view, mine or use data is not far behind. Not a good result if data protection is the goal.

The problem is that, assuming a "moment in time" or any other deterministic number is used as a seed, that moment in time is fixed, that is, it is a real number, picked from a real, albeit difficult to predict or determine, system (the clock on a computer or some other stream of data). At the time of capture, though that number is fleeting and may be measured in a very small unit, it can still be determined no matter how small the unit, because it is fixed, deterministic.

If commercial companies only had to worry about data protection and not Government restrictions on the export or import of encryption products, a company could randomly manipulate the seed in order to create unbreakable or nearly unbreakable encryption and create a cost efficient, commercial computer and related programs for worldwide distribution containing unbreakable crypto. A few examples, some more farfetched than others:

1. Could you imagine if your commercial computer was equipped to detect the number of dust particles in the air, or any measurable airborne particle, pollutant, moisture particle, condensation (jointly "particle"), in or near it, at the time you called upon it to perform a cryptographic function and it used that "particle count" as the basis for a seed?

2. Or, if your commercial computer could detect the number of such particles once and then do likewise one-nano second later and use some random changing multiplier creating a sum, based on a changing arithmetic equation, and then the crypto system in your computer used that sum as a seed?

3. Or if the seed was created based on a bacteria count or any airborne contaminant particle count near your computer?

4. Or if the seed was created based on a particle count from a light source shining on your monitor

Considering these examples, the seed would be so random, so dynamic and so unpredictable at any given time that breaking a crypto code would be too time consuming even using the strongest, most high powered computer system, virtual or otherwise. The seed would be nondeterministic. It does not matter what the particle count to create the seed might be based on so long as it is dynamic and random.

Many Governments and high level engineers from academic institutions throughout the world already have this simple concept in place and have created usable nondeterministic seeds but cannot commercialize the detection and seed creation process because the related commercial product would be solely for domestic use. Under present export and import regimes around the world, the commercial product would not be exportable or importable without a license, and in some countries without a mechanism in place to divulge the seed or the process to capture it. If commercialized, some countries might even block export and import, period.

Two additional problems to be addressed: First, including detection hardware and software in a computer necessary to capture a particle count to create a nondeterministic seed might make the computer unmarketable from a price viewpoint, though sensors capable of performing such a particle count already exist and are reasonably priced. Second, the operation of the detection hardware and software necessary to create a nondeterministic seed may not be as efficient, thereby overburdening the processor, or as fast in relation to most crypto presently available on the market. A tradeoff might have to be made in favor of more security at the expense of price and efficiency.

If the Governments and institutions working with nondeterministic seeds as the basis for cryptography were unleashed to create and commercialize crypto based on the concept mentioned in this article, without concern for world-wide export and import regulations, Governments, hackers, cyber criminals, or intruders would never be able to break crypto code again, for better or worse.

Dan Minutillo has practiced law in Silicon Valley for over 35 years. His practice is limited to export, import, and Government contract law. The Firm has represented many of the largest public and private companies in Silicon Valley and it is on the cutting edge regarding encryption technology. Dan has taught for UCLA, the University of Santa Clara Law School and their MBA program, at Stanford University for the NPMA, lectured to the World Trade Association, and he received the Silicon Valley Service Provider of the Year Award. Dan has been published nationally and regionally. dm@hogefenton.com www.hogefenton.com