Lawful Access and Security: A Transatlantic Perspective – EastWest Institute

Statement by Prof. Dr Udo Helmbrecht, ENISA Executive Director

THE HAGUE

19TH- 20TH MAY, 2016

Einstein: "Insanity: doing the same thing over and over again and expecting different results." In this spirit, I would like to reflect on laws that limit the free use of cryptographic tools. Several attempts of such rules were made. The success was at most mixed, the negative impact on the other hand was sometimes huge.

Here, I would like to reflect on one prominent example: the US export regulation for crypto.

The United States Government classified cryptographic algorithms as Auxiliary Military Equipment in the US Munitions List. The use of strong encryption by software developed in the US was only allowed on US soil. Outside of the US, only weak variants of the encryption routines were allowed. As an immediate result, for example, Netscape developed two versions of its web browser. The "U.S. edition" supported full size RSA public keys in combination with full size symmetric keys. (At the time this was 1024bit RSA and 64bit symmetric, today that would be 4096bit and 256bit symmetric). While the "International Edition" had its effective key lengths reduced to 512 bits and 40 bits respectively. Interestingly, this even lowered the protection level in the U.S., since acquiring the 'U.S. domestic' version turned out to be sufficient hassle that most computer users ended up with the 'International' version. A similar situation occurred with Lotus Notes.

Now in a fast moving market like IT, one would expect the ruling has no impact anymore. But surprisingly, although the policy was changed (and mostly abolished) 15 years ago, today it has still an impact on security. Namely, the FREAK[1] and Logjam[2] attacks both have used legacy code that was only included in the systems because of the afore mentioned regulation.

Further, more subtle effects have been observed. In 1999 the U.S. Senate Committee on Commerce, Science, and Transportation collected information on the development of cryptographic products outside of the U.S. It was found that the foreign market was rapidly growing and that the quality of the offered products is at least at par with those from U.S. based companies. The testimony further suggests that U.S. export regulations did in fact damage IT industry.

From these two observations I would conclude: It is the responsibility of the policy makers to pass laws that are just, equitable. The legal framework should have the least impact on peoples' and industries' freedom. Moreover, public policy tends to last for a long time. Computing costs are systematically decreasing, in ever shorter periods. Therefore, attacks that seem out of the reach of any one but a nation state will not remain so for the lifetime of the implementations. As such, policy makers

- Shall refrain from limiting in any way security features in computer software
- Shall refrain from limiting in any way the export of security features in computer software
- Shall consider lifting any and all existing limitations for security features in computer software

Otherwise, history will repeat itself: vulnerabilities that where left from legacy policy will be abused to attack systems. Further, policy that limits the use of cryptography in commercial products will again damage IT industry.

[1] "FREAK: Factoring RSA Export Keys," K. Bhargavan et al. [Online]. Available: https://www.smacktls.com/#freak last accessed in May 2016.

[2] "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice" David Adrian et al. [Online]. Available: https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf last accessed in May 2016.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu