The Risk of Secrecy in Governmental Cybersecurity Program : Case Study of the Einstein Project

Charlotte Clément-Cottuz

This paper argues that the over-secretive nature of cybersecurity national programs that protect national agencies actually hinders such programs while it demonstrates that a more transparent implementation could enhance its efficiency. This argument can appear paradoxical as logically the more transparent a cybersecurity program is, the easier it can be for hackers to find loopholes in these programs and thus to perpetuate their malicious intents. However, based on the case study of the US Einstein program, this paper demonstrates that the shortcomings of such programs are majorly caused by unnecessary exaggerated secrecy.

Einstein, or formally called the US National Cybersecurity Program System, was developed by the United States Computer Emergency Readiness Team (US-CERT) which is the operational arm of the National Cyber Security Division of the US Department of Homeland Security (DHS). This department "has the mission to provide a common baseline of security across the federal civilian executive branch and to help agencies manage their cyber security risk" (CDT, 2009). Internationally, national governments have implemented similar programs to defend their national organisations against cyber offensives. For example, in France, the ANSSI (Agence Nationale de la Sécurité des Systèmes d'Informations) ensures the cybersecurity of national public and private sector operators. Nevertheless, confronted with the lack of information concerning the digital control and supervisory control and data acquisition systems (DC/SCADA) put in place by the ANSII (Dila, 2013) or other national governments across the globe, this post focuses on the US and its Einstein program.

More precisely, Einstein was developed to fulfil two key roles in federal government cybersecurity. First, as an intrusion detection capability, it detects and blocks cyberattacks from compromising federal agencies by monitoring these federal agencies internet connections for specific predefined signatures of know malicious activity and anomalies and alerts US-CERT when specific network activity or host-based intrusions match the predetermined signatures are detected. Second, Einstein was enhanced to also become an intrusion prevention capability that automatically blocks malicious traffic from entering or leaving the federal civilian executive branch agency networks. To this extent, Einstein has the capability of analysing the content of emails and other Internet websites (Gorman, 2009). This raises massive privacy questions. Indeed, there are no clear or transparent guidelines made public about Einstein's exact mission, who reads these emails, what are the tools implemented against cyber threats and which precise cyber threats are encompassed in such a vast definition (CDT, 2009). Therefore, the US-CERT and the DHS profit from a lot a legal leeway when they are questioned or held accountable and overall they benefit from this lack of transparency (Gao, 2010) at the expense of the Einstein users.

On top of the privacy risks caused by the lack of transparency, the latter also impairs on Einstein's efficiency. Indeed, another role of Einstein is cross-collaboration between the

agencies: once an agency acknowledges an intrusion/signature/zero day, it alerts the US-CERT which then informs the other agencies of the newly determined intrusion. Therefore like a network effect, the more agencies using Einstein and hence finding signatures and exchanging them, the higher is Einstein's global success rate. However, Einstein is only implemented in 5 agencies out of 23 because each agency implements different technologies to protect its sensitive data that are not compatible with the Einstein program. Therefore, the lack of transparency between federal cybersecurity programs impairs on the effort of the federal Einstein program and diminishes its efficiencies. Indeed, during a test to flag a portion of vulnerabilities associated with common softwares applications across multiple federal agencies, only 6% of all the security bugs tested were found. That's 29 out of 489 vulnerabilities (Paganini, 2016). If more transparent, Einstein's would be easier to implement and hence more efficient.

Finally, the efficiency shortcomings of the Einstein program could be straightened up by informing the federal employees whose computers are running the Einstein program. Indeed, over-preoccupied by the secrecy of the program, the DHS did not inform the federal employees whose computer were running the program. However, if the US-CERT simply informed the employees that the program is running, communicated on the EINSTEIN program, employees would be more aware and careful of malwares and phishing tentatives. Furthermore, if the US-CERT encouraged cybersecurity awareness programs, it would definitively increase the efficiency of Einstein. And to a certain extent, "agencies should ultimately employ a multi-layered approach to security that includes well-trained personnel, effective and consistently applied processes, and appropriate technologies" (Cooney, 2015).

Even though it is being amended, Einstein raises serious concerns of transparency. Its lack thereof causes privacy contingencies but also inefficiencies and failures, which can endanger the US national sovereignty to a certain point. However, a more transparent implementation with more thorough information concerning the program communicated by the US-CERT would increase the number of federal agencies relying on the Einstein program and hence its capability. Furthermore, at the grass roots level or in other words at the user level, awareness and communication on the EINSTEIN program would increase the number of signatures detected and hence once again EINSTEIN's efficiency. In a few words, transparency is the best policy.

References

CDT, 2009. 'Einstein Intrusion Detection System: Questions that Should be Addressed', Center for Democracy & Technology, July 2009, Available at https://www.dhs.gov/einstein

Dila, 2013, Direction de l'information légale et administrative. Livre Blanc Défense et Sécurité Nationale, 2013. Available at <http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf >

Gorman, S. 2009. 'Trouble Plague Cyberspy Defense', Wall Street journal, July 3rd 2009,

CDT, 2009. 'CDT report : Privacy, Legal Concerns Surround Secret Government Cybersecurity System', CDT, July 28, 2009.

Gao, 2010. 'Cybersecurity: Progress made but challenges remain in defining and coordinating the comprehensive national initiative', Report to Congressional Requesters, March 2010. (note: In 2010, the United States Government Accountability Office (GAO) published a report that demanded that 'an appropriate level of transparency' to be applied to Einstein)

Paganini, P. 2016. 'Audit shows Department of Homeland Security 6 billion U.S. Dollar firewall not so effective against hackers', Security Affairs, February 1, 2016.

Cooney, M. 2015. 'GAO: Early look at fed's "Einstein 3" security weapon finds challenge', Network world, July 9th 2015.