Long-term data security challenges using cloud storage services

Martin Brehmer, Jürgen Seitz

Angaben zur Veröffentlichung / Publication details:

Brehmer, Martin, and Jürgen Seitz. 2015. "Long-term data security challenges using cloud storage services." In *WHICEB 2015 Proceedings - Fourteenth Wuhan International Conference on e-Business, Wuhan, China, June 19th-21th, 2015*, 21. New York, NY: AIS Electronic Library (AISeL). https://aisel.aisnet.org/whiceb2015/21/.

Summer 6-19-2015

Long-term Data Security Challenges Using Cloud Storage Services

Martin Brehmer
Baden-Wuerttemberg Cooperative State University Heidenheim, Germany

Juergen Seitz
CANCOM SE, Germany, seitz@dhbw-heidenheim.de

Long-term Data Security Challenges Using Cloud Storage Services

Martin Brehmer[1,2], *Juergen Seitz*[1*]
[1]Baden-Wuerttemberg Cooperative State University Heidenheim, Germany
[2]CANCOM SE, Germany

Abstract: The relevance of cloud computing, especially cloud storage services, was growing steadily within the last years. By getting more acceptance from customers, there are several new issues coming up, especially the question of data security. Therefore this paper analysis impacts on data security in the future, based on recent encryption methods like AES and TLS used in combination with RSA, on a non-calculation perspective and without taking into account key exchange methods like Diffie Hellman. This paper discusses why it is important to think about data security issues right from today.

Keywords: cloud computing, cloud storage services, data security, data privacy, confidentiality, data encryption

1. INTRODUCTION

According to a report about top technology trends in 2014 of Gartner three of ten technology trends include the word 'cloud'. Another Gartner report from October 2014 states that "cloud computing is driving a new wave of services that are displacing traditional business processes" [1]. IDC assumes that the market for cloud services will increase within the next five years dramatically [2]. In summary, cloud related technologies and services will dominate digital business and information technologies the next few years.

Using new information technologies nowadays lead corporate objectives on a long term perspective. This means in particular that these technologies have to be carefully analyzed relating to possible major strategic effects, advantages and disadvantages, which sometimes can hardly be measured. Economic advantages and disadvantages of an information system may differ by the strategic alignment of each company and their usage of technologies. In case of further strategic effects there is a question of IT compliance, which means that the use of IT infrastructure is in accordance with laws, the corporate policy and other relevant rules such as data security or IT risk management issues for instance. The need of IT compliance is a logical conclusion because otherwise non-compliance would lead to legal and/or security risks and costs [3]. As a consequence for an effective use of new technologies analyzing economical, also technological benefits and impacts, as well as the consideration of IT compliance, is important and of course a complex procedure. The use of an upcoming technological issue like cloud, cloud computing or cloud services requires a business, IT compliance and an IT security concerning analysis. Therefore, this paper analyzes recently used data protection technologies, be implemented using encryption methods in the special case of cloud storage services on a long term perspective as a kind of preparation to possible upcoming IT compliance and IT security issues.

2. THE NEED OF ENCRYPTION IN CLOUD ENVIRONMENTS

The National Institute of Standards and Technology (NIST) has defined cloud computing as a model to enable conveniently on-demand network access to a shared pool of configurable computing resources "(e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models." [4] This means cloud computing is an on-demand service model to get simple and fast access to distributed computing resources and

* Corresponding author. Email: seitz@dhbw-heidenheim.de

services via a network based on three service models called Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

Thus, regarding to a cloud storage service perspective, IaaS can be used to get access to a provided infrastructure, a storage solution for instance. But a cloud storage solution includes an opportunity to use SaaS, too. In this case the provided software could be a file sharing system based on any network attached storage. Both principles together are often advertised and sold as one solution like from Dropbox, Box or Google [5] [6] [7]. The access to the cloud storage services itself can be provided by three different types of architectures called private, public or hybrid cloud. A private cloud is based on a system architecture where the customer takes responsibility for software and management issues and the needed local infrastructure. In comparison a public cloud is provided by an external service provider who assumes most of the responsibility. In this case infrastructure is externally located. Hybrid cloud architecture is an on premise infrastructure which is managed by an external service provider [8]. That means by using cloud storage services it is not necessary to know where the storage infrastructure is exactly located. At first this seems to be no problem, but at second glance questions are coming up with regards to important confidential data. There exist several levels of confidentiality of data in companies. Therefore a company has to classify their data and define activities to guarantee the confidentiality. Examples for sensible data are personal information, but also knowledge of a company like construction plans, data which should not be stolen like credit card information, be copied, seen by a third party or simply get lost. For instances, a loss of data could also lead to a high corporate financial damage in case of new ideas which will be then patented by a competitor. Therefore, it is necessary to have a long-term protection for data especially in the cloud and the transfer of data into the cloud.

3. TRANSPORTATION AND STORAGE ENCRYPTION OF CLOUD SERVICES

In order to analyze the level of confidentiality of data in a cloud environment the aspects of data transportation and data storage have to be considered. Nowadays data encryption is widely used for data transportation. Usually the transported data are only useful and valuable for a very short time, e. g. online banking data. A TAN can be used only once and after the transaction is cleared the TAN is useless. In contrast, data transmitted to the cloud and stored in the cloud are usually documents which are useful and valuable for a longer time. In 2014 most of the providers in the area cloud storage services business like Dropbox, box and Amazon web services are using AES 256 Bit encryption as a local data encryption algorithm and a SSL-/TLS-tunnel for a secure transportation of data [9] [10] [11] [12].

Encryption algorithms and protocols have been changed from time to time due to revealed security gaps or new arisen technological possibilities like more computing power or better cracking tools. So, for the forecast on security issues of cloud storage services it is necessary to take into account recently known and past security gaps or vulnerabilities of used encryption methods. Beginning with the transport security, the security of the SSL/TLS protocol has to be investigated because there have been lots of security leaks [13]. In 2014 two popular security leaks have been revealed. The first one was the security leak called ‘Heartbleed’, which was a “catastrophic bug in Open SSL” [14]. This bug enables attackers to get access and to encrypt data traffic. Regarding to cloud storage services this means that all the data which where transmitted could be misused. This was a big blow for the trust of customers not only in cloud storage services but even in e-business in the point of online shops or online banking. The second revealed big leak in the SSL/TLS protocol was “Poodle”. With Poodle an attacker was able to get simply access or even able to crack encrypted data communications by using an SSLv3 backdoor [15]. Heartbleed has been active for about 3 years and Poodle for over 15 years, which especially means, that SSL/TSL has been unsecure for that time and this is hardly unimaginable from a security perspective. In view of the used encryption protocol of SSL/TLS, RSA algorithm has to be analyzed. In 2013 Genkin et al. published a paper on cracking 4096

bit RSA encryption which has been the first known successful attack of RSA encryption algorithm based on 4096 bits. This attack works by using microphones to listen to computer noises caused by vibrations during the decryption process. There is to mention that even cellphone microphones are sufficient for a successful attack, but that also means that the listener has to be close enough to the victim or even need a backdoor in another computer system like a cellphone [16]. A few years before in 2010, Pellegrini et al. published a paper on cracking 1024 bit RSA encryption within round about 100 hours. This again has not been a mathematical decryption attack; instead they exploited error caused vulnerability. In detail, they caused an error by manipulating the processor, which handles the decryption key through submitting transient varying voltages. With the information of these faults hackers were able to extract the private key, so they could decrypt the communication, which is again quite bad for common trust in encryption protocols [17].

The story of AES encryption starts in the summer of 1999, when the DES (Data Encryption Standard) was cracked the first time by a brute force attack. Since the release of AES, it is still one of the most popular symmetric encryption algorithms [18]. In 2011, there have been some rumors that the AES encryption is cracked. This wrong statement was caused by an article in an online magazine called 'the INQUIRER' [19]. The article itself bases on a paper of Boddanov et al. (2011), but in comparison to the article in the magazine they did not say that they are absolutely able to crack AES encryption, they just show AES vulnerability. In this case of course the detection of an AES encryption vulnerability has been an impressive progress in cryptography, but according to the result of this paper it does not have a real impact, for instance the authors themselves state that it won't "threaten the practical use of AES in any way" [20]. In the same year Biryukov et al. (2011) also published a paper about cracking AES encryption by a hypothetical supercomputer, called 'CAESAR', which is based on GPU (Graphic Processor Unit) computing power through a hypothetical use of NVIDIA GT200b graphics chips. The result of this paper is, that e.g. by using two different attacks the time to crack an AES-256 encryption would take about one year for the first (called "Related-Key Cryptanalysis" attack), and about one month for the second (called "Time-Memory-Key") sort of attack. But if CAESAR is used in practice, it would definitely have its limitations, so for instance as a result they say that this kind of supercomputer has mainly two bottlenecks, the first and most important is the power consumption of CAESAR with about 4TW, which is higher than the power consumption of the whole United States of America in 2005. Second there are limitations for graphics chips production and the related production costs [21]. So in total we can assume that cracking AES encryption could be possible with such a supercomputer but possibly not on the basis of current technology.

According to the news of the last two years, there have been some upcoming security issues, caused by Edward Snowden, who released some classified NSA documents about digital surveillance through the United States of America [22]. Since then, also the AES encryption is a doubtable encryption algorithm. Schneier wrote in his blog as an answer to the question if the NSA is able to crack AES encryption: "My guess is that they can´t". He explains that in his point of view there is no available attack to crack AES in a certain realistic time. Rather they will find possible methods to bypass the encryption algorithm than to crack it [23]. In a recent conversation of Snowden and Schneier at Harvard Data Privacy Symposium both agree that the biggest security gaps seem to be the implementation of security methods, such as SSL/TLS or AES and not the encryption method itself. These gaps can be exploited by the NSA and even other hackers, too [24].

As a summary we can say that, at the moment, the SSL/TLS protocol, according to the recently revealed security leaks, is not that safe than it is often advertised, because it strongly depends on the implementation of the protocol. Also the use of the RSA encryption method is not that safe anymore, but we can assume that this case only will take effect upon highly confidential classified documents, because it takes some effort to get access to the data. On the safety of the AES encryption we can state that right now, it looks like it is one of the strongest

symmetric algorithms, which means it can be assumed as secure. Transferred to cloud storage services there is to mention that, in particular, a selection of a specific cloud storage service provider should not be an overhasty act, because to be mostly secure, an investigation of the implementation of the security mechanisms is necessary. For that also the architecture of the cloud storage service provider should be taken in account. As a given fact, related to the architecture itself and the mentioned security issues in the point of implementation, we can state that cloud storage services, especially for companies, should be based on a private, which is the most secure, or a hybrid cloud architecture, which reduces disadvantages of private and public cloud architectures to achieve a higher level of data security.

4. IMPACTS FOR DATA SECURITY OF CLOUD STORAGE SERVICES

To order to analyze impacts for data security of cloud storage services assumptions have to be made to different scenarios. According to the previous findings it can be assumed that the security of encryption methods in future is related to:

- Progress in the area of crypto analytics
- Progress in finding backdoors/in bypassing security mechanisms
- Technological progress for brute force attacks

Regarding to a possible progress by consideration of the past we can assume that there is perhaps a progress in RSA decryption but not in AES decryption. We can also assume that there are still some unknown backdoors by using SSL/TLS encryption or especially by an incorrect implementation of this protocol, which is unknown yet. Looking at brute force attacks, these attacks which always work on any kind of block cipher encryption need a lot of time [25]. For that reason we can assume that reducing time for brute force attacks by faster technology, i. e. better computing power, is a big factor. To make predictions of impacts for security of encryption algorithms, research in the area of technological progress of computing power is necessary.

In 2013, Nagy et al., has shown that Moore's law is probably one of the best indicators on technological progress [26]. Schaller assumed in 1997 that Moore's law, which has first basically predicted that density of components, e. g. on a CPU or GPU, will double every 18 months (a revised number of the first predicted 12 months), looks like it could be transferred to computing power [27]. By taking into account that Biryukov et al. used a "GT200b" graphic processor (released in June 2009) for their theoretical supercomputer 'CAESAR' the same theoretical supercomputer with currently used graphic processors should be able to use more cores on one graphic processor for calculation. In November 2013, Nvidea Corp. released a graphic processor called 'GK110B', which has the biggest number of implemented cores on an Nvidea graphic processor till today. In a direct comparison of these two graphic processors, there is an increase from 250 cores on a 'GT200b' up to 2880 cores on the 'GK110B' model. According to Moore's law the total number of cores of a current graphic processor has to be bigger (round about 3090 cores, calculation based on doubling of components in 18 months), but in consideration of time compared to the increasing development of cores, a difference of round about 210 cores is not much. But regarding to limitations of 'CAESAR', one of the physical bottlenecks is power consumption. GT200b needed 204W while GK110B requires 250W in total of all cores [28] [29] [30]. This means that there is a power consumption of 0,85W per core for the older graphic processor and 0,087W per core for the newer model. Compared to the increase of cores the decrease of power consumption per processor is much higher [31]. Taking into account that power consumption per core decreased by a factor of nearly 10 in less than six years and there is still a potential to decrease further, it can be assumed that this will have an effect on hypothetical supercomputer like 'CAESAR'. This means that further research on supercomputers based on the assumptions of Biryukov et al. compared with newer technology will be interesting to get a more detailed future perspective [32]. At the moment, it can be stated that currently used

technology still doesn't allow effective and efficient cracking of AES encryption because of power consumption limitations.

The research of Wineland and Haroche on quantum computers could imply progress in the area of decryption and also in cracking of encryption algorithms. Publications of Snowden are also a sign that there already methods exist [33] [34]. According to Schneier at the moment quantum computers for cracking encryption methods are not available, even not for the NSA, and it will take more years to develop a computer based on quantum technology [35].

It can be summarized that regarding to transportation security implemented using SSL/TSL protocol it is possible that further protocol related vulnerabilities and also some backdoors caused by incorrect implementation come up. Furthermore, cracking encryption methods is possible in some cases, but there will be a restricted effect on the security of cloud storage services by using RSA 2048 or higher, because the complexity is very high. Considering the analyzed security aspects related to AES encryption it can be assumed that data, encrypted with this algorithm, is secure today, but on a long term perspective there is a risk that AES could be decrypted or cracked, probably not in the next one or two years, however, in a foreseeable period of several years. At this point it also should be mentioned that, according to heise, the NSA is storing data from the Internet to decrypt it in the future [36]. Thus, especially on a perspective of a long term use of cloud storage services it can be stated that providers who are storing valuable, sensible data or data, which are stored today for prolonged use with a low frequency of access, will be carefully selected by corporate customers.

5. CONCLUSIONS

In this paper currently used encryption algorithms and protocols used by cloud storage providers have been analyzed. It can be summarized that the level of data security and confidentiality today is mostly related to the current implementations of security mechanism like SSL/TLS protocol and unknown vulnerabilities. Therefore, a cloud storage service provider and its used architecture or security mechanisms should be carefully investigated before signing a service contract by a customer. Particularly noteworthy is that a private cloud or hybrid cloud infrastructure is the best choice for corporations to store their data securely in a cloud infrastructure. On a long term perspective everything, which is encrypted and stored today has to be monitored. In the long run data are not secure in a network environment. Even continuous observation of currently used data security mechanisms doesn't guarantee security and confidentiality of data.

ACKNOWLEDGEMENT

This research was supported by CANCOM SE, Erika-Mann-Str. 69, 80636 Munich (Germany).

REFERENCES

[1] Clearly D. W. (2014). The Top 10 Strategic Technology Trends for 2014, Document-Nr. G00260410.

[2] Gens F., IDC Global IT Public Cloud Services Forecast Team (2014). Worldwide and Regional Public IT Cloud Services 2014–2018 Forecast, Document-No. 251730.

[3] Johannsen W., Goeken M. (2006). IT-Governance – neue Aufgaben des IT-Managements. HMD - Praxis der Wirtschaftsinformatik, 250: 7-11.

[4] Mell P., Grance T. (2011). The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. US National Inst. of Standards and Technology; Special Publication 800-145: 2-3.

[5] Dropbox Inc. (2015). Dropbox Homepage. https://www.dropbox.com/business/why-dropbox-for-business/, accessed on 04.02.2015.

[6] Box Inc. (2015). Products and Features. https://www.box.com/business/products-and-features/, accessed on 04.02.2015.

[7] Google Inc. (2015). Google Drive. https://www.google.com/intl/en/drive/, accessed on 04.02.2015.

[8] Plass C., Rehmann F. J., Zimmermann A., Janssen H., Wibbing P. (2013). Chefsache IT. Wie Sie Cloud Computing und Social Media zum Treiber Ihres Geschäfts machen. Berlin, Heidelberg et al.: Springer-Verlag , 39-41.

[9] Griffith E. (2014). Who's winning the consumer cloud storage wars? http://fortune.com/2014/11/06/dropbox-google-drive-microsoft-onedrive/, accessed 04.02.2015.

[10] Dropbox Inc. (2015). Your stuff is safe with Dropbox. https://www.dropbox.com/security/, accessed on 04.02.2015.

[11] Box Inc. (2015). Redefining Security for the Cloud. https://www.box.com/business/enterprise-security/, accessed on 04.02.2015.

[12] Amazon Inc. (2015). Amazon S3 Details. http://aws.amazon.com/de/s3/details/#security/, accessed on 04.02.2015.

[13] Open SSL Development Team (2015). OpenSSL vulnerabilities. http://www.openssl.org/news/vulnerabilities.html, accessed on 04.02.2015.

[14] Schneier B. (2014). https://www.schneier.com/blog/archives/2014/04/heartbleed.html, accessed on 04.02.2015.

[15] Schmidt J. (2014). Der Todesstoß für SSLv3. c't 2014(24): 50.

[16] Genkin D., Shamir A., Tromer E. (2013). RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. Berlin, Heidelberg et al.: Springer-Verlag, 444-461.

[17] Pellegrini A., Bertacco V., Austin T. (2010). Fault Based Attack of RSA Authentication. IEEE: 855-860.

[18] Beutelspacher A, Neumann H. B., Schwarzpaul T. (2010). Kryptografie in Theorie und Praxis. Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld. Wiesbaden: Vieweg+Teubner, GWVFachverlage GmbH, 81,88.

[19] Neal D. (2011). AES encryption is cracked. Researchers find a weakness in the algorithm. http://www.theinquirer.net/inquirer/news/2102435/aes-encryption-cracked/, accessed on 04.02.2015.

[20] Bogdanov A., Khovratovich D., Rechberger C. (2011). Biclique Cryptanalysis of the Full AES. Berlin, Heidelberg et al.: Springer-Verlag, 344-371.

[21] Biryukov A., Großschaedl J. (2011). Cryptanalysis of the Full AES Using GPU-Like Special-Purpose Hardware. Amsterdam: IOS Press, 221-237.

[22] Snowden E. (2014).Free Snowden – The Courage Foundation Homepage. https://edwardsnowden.com/de/, accessed on 04.02.2015

[23] Schneier, B. (2014). Can the NSA Break AES? https://www.schneier.com/blog/archives/2012/03/can_the_nsa_bre.html, accessed on 04.02.2015

[24] Schneier B., Snowden E. (2015). Bruce Schneier and Edward Snowden @ Harvard Data Privacy Symposium 1/23/15. https://www.youtube.com/watch?v=7Ui3tLbzIgQ&feature=youtu.be, accessed on 04.02.2015

[25] Beutelspacher A, Neumann H. B., Schwarzpaul T. (2010). Kryptografie in Theorie und Praxis. Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld. Wiesbaden: Vieweg+Teubner, GWVFachverlage GmbH, 67-68.

[26] Nagy B., Farmer J. D., Bui Q. M., Trancik J. E. (2013). Statistical Basis for Predicting Technological Progress. PLOS ONE Journal 8(2): e52559, doi: 10.1371/journal.pone.0052669.

[27] Schaller R. R. (1997). Moore's law: past, present, and future. IEEE Spectrum Journal, 34(6): 53-55, 59.

[28] Biryukov A., Großschaedl J. (2011). Cryptanalysis of the Full AES Using GPU-Like Special-Purpose Hardware. Amsterdam: IOS Press, 221-237.

[29] NVIDEA Corp. (2015). Grafikkarte GeForce GTX 780 Ti. http://www.nvidia.de/object/geforce-gtx-780-ti-de.html #pdpContent=2/, accessed on 04.02.2015.

[30] Wallossek I., Angelini C., Strömer G. (2013). Nvidia GeForce GTX 780 Ti: GK110, endlich komplett - muss Titan dran glauben? http://www.tomshardware.de/geforce-gtx-780-ti-review-benchmarks-grafikkarten-gpu,testberichte-241425.html, accessed on 04.02.2015.

[31] Schaller R. R. (1997). Moore's law: past, present, and future. IEEE Spectrum Journal, 34(6): 53, 55.

[32] Biryukov A., Großschaedl J. (2011). Cryptanalysis of the Full AES Using GPU-Like Special-Purpose Hardware. Amsterdam: IOS Press, 221-237.

[33] Heise online (ed.) (2012). Physik-Nobelpreis geht an Quantencomputer-Pioniere. http://www.heise.de/newsticker/meldung/Physik-Nobelpreis-geht-an-Quantencomputer-Pioniere-1726274.html, accessed on 04.02.2015.

[34] Rich S., Gellman B. (2014). NSA seeks to build quantum computer that could crack most types of encryption. http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html, accessed on 04.02.2015.

[35] Schneier B. (2015). What Exactly Are the NSA's 'Groundbreaking Cryptanalytic Capabilities'? http://www.wired.com/2013/09/black-budget-what-exactly-are-the-nsas-cryptanalytic-capabilities/, accessed on 04.02.2015.

[36] Weber D. (2014). Alles ist geknackt ...alles? Nein! http://www.heise.de/security/artikel/SSH-SSL-IPsec-alles-kaputt-kann-das-weg-2514013.html, accessed on 04.02.2015