ENCRYPTION: MYTHS AND REALITIES

Montreal, September 2013
René W. Vergé, CEO and Co-Founder, VoD2

"Our entire information society rests on a fragile foundation that mathematicians are racing to dismantle."[i]

SUMMARY

The purpose of this white paper is to demonstrate that encryption is not the miracle solution that it is purported to be[ii]. The vast majority of stakeholders generally believe that encryption is the ultimate measure that will ensure total security and privacy of your information. This is a myth. Although encryption, when used properly, can often reduce privacy and confidentiality risks, it is often a smoke screen fraught with obstacles and does not address the true problem.

We hope that this white paper will generate further discussion on the subject. What's happening today with the Internet, cloud computing, mobility, social media, global surveillance and the international legal landscape is unprecedented. Whether encrypted or not, your data is frequently misused, accessed by a large number of people and companies, transferred to subcontractors and surrendered to third parties, without your knowledge or consent. In this context, relying solely on encryption to ensure confidentiality and privacy is a risky proposal and, ultimately, a recipe for disaster.

Although some of the arguments brought forward in this white paper may be of a technical nature, we have simplified them as much as possible to present them in layman terms. More information can be found in the references listed at the end of this white paper.

1. Encrypting data does not ensure its integrity or availability

It is commonly known that information security is achieved when 3 conditions are met: Confidentiality, Integrity and Availability of your data. Encryption can often reduce confidentiality risks, but it does not ensure that your data will maintain its integrity or be available when you need it. Hashing algorithms like MD5 will detect a loss of integrity, but they will not ensure it.

Other security measures, therefore, will have to be deployed to address those requirements. For example, backup copies still have to be performed by the user and by the storage and service providers to ensure availability of your data.

Because of the distributed nature of the Internet, more specifically the cloud, these security measures are implemented by different service providers, with varying degree of reliability and effectiveness, in various geographical locations. There is no coordination between all these providers and you have no guarantee whatsoever that these security measures are adequate or working properly. Your information therefore is more vulnerable and at greater risk.

In fact, encryption may even hamper information availability and render it inaccessible permanently if encryption keys are changed, lost or corrupted[iii].

2. Encrypting data may not prevent it from being stolen

Data encryption may not protect your data from theft or disclosure. For example, if Full Disk Encryption is used at the hardware or storage array level, data will only be protected when the disks are powered off. As soon as the disks are powered up by an authorized user, the data on them is decrypted and available to anyone that can connect to the disk volume[iv].

On the other hand, additional protection may be achieved within the network environment, for example if Network Attached Storage (NAS) or Storage Area Networks (SAN) encryption is used, but all other traditional security measures are still required and become critical within the data centers[v]. Furthermore, cloud services often implement encryption within their infrastructure using encrypted volumes, which use the same username/password or private key to encrypt all customer data[vi]. Once someone has unlocked it, they have access to all the data on the drive.

Encryption during data transport, using Transport Layer Security (TLS/SSL), on the other hand, protects only at the edge of the cloud, leaving traffic between servers and within data centers exposed[vii].

Regardless of which service provider you use or how encryption is deployed, you become dependent on an environment that you do not control. In the cloud, this problem is exacerbated since you often do not know where your data is located or which service provider or other third party has access to it.

3. Encryption in general is very complex

Cryptography is harder than it looks[viii]. What Bruce Schneier wrote in 1998 in "Security Pitfalls in Cryptography" still holds today:

> *"A cryptographic system can only be as strong as the encryption algorithms, digital signature algorithms, one-way hash functions, and message authentication codes it relies on. Break any of them, and you've broken the system. And just as it's possible to build a weak structure using strong materials, it's possible to build a weak cryptographic system using strong algorithms and protocols."*[ix]

There are many examples of poor implementation of cryptography, including products that have been certified under the well known NIST FIPS 140-2 standard[x], numerous cryptographic products developed by the world's largest software company[xi] and many other products[xii].

4. Encryption in the Cloud is even more complex

Encryption in the cloud can be implemented at different levels: 1) data-in-motion, including encrypted communication channels between user or organisation and service provider, between provider and sub-contractor, between web servers and application servers, between application servers and databases, between networks, etc.; 2) data-at-rest, including disk encryption, record encryption, device encryption, backup and archive encryption, etc. and 3) data-in-process, including virtual machine encryption (although there is no way currently, nor likely in the near future, to deal with the processing of encrypted data)[xiii].

Each level on encryption comes with its advantages, disadvantages and risks. Encryption keys themselves have to be managed and secured, often over long periods of time. Because by nature the cloud is distributed and generally involves many providers, sometimes in different geographical locations, the user or the organisation most often does not know where his data is processed, communicated or stored[xiv].

Although some cloud security providers have come up with innovative solutions[xv], the fact remains that encryption processes in the cloud are very complex and the risk of failure and data breaches can be much greater than in traditional hosting environments.

5. Managing and protecting encryption keys is difficult

Managing and protecting encryption keys is a major challenge, especially in the cloud. Once data is moved to the cloud and virtual environments, the question becomes “who do I trust?" If you rely on encryption to protect your data, who can you trust with the encryption keys?

One option is to store the keys in the cloud, either on the same cloud infrastructure you use for your data, or with a dedicated key management vendor. Doing this means that you trust the chosen provider to keep your keys safe. Recent security incidents however confirm that security providers themselves are exposed to attacks (VeriSign[xvi, xvii, xviii], RSA[xix, xx, xxi], Symantec[xxii, xxiii, xxiv], Digicert[xxv, xxvi, xxvii]). Therefore, many will argue that you should trust no one with your encryption keys.

The other option therefore is to store the encryption keys on your own premise[xxviii]. That approach however may defeat the purpose of moving to the cloud in the first place, since an infrastructure deployment will still be required on your own premise or back in the data center. More often than not, this will result in an expensive solution, as well as the loss of important cloud advantages such as scalability and elasticity[xxix].

6. Someone else may have access to the decryption keys

You are never certain that someone out there does not possess the decryption keys for your encrypted data. The encryption technology supplier, the service provider, a sub-contractor of the supplier, an employee, a government agency, a hacker or anyone else can have access to or possess the decryption keys. You have no real way to confirm or deny this.

In fact, recent events and revelations tend to confirm that many people out there have access to decryption keys when they shouldn't, often without the knowledge or consent of the data owner (Apple[xxx], Sony[xxxi], NSA[xxxii], FBI[xxxiii]).

Because of the distributed nature of the cloud, it is very difficult, if not impossible, to confirm that decryption keys, including master keys will not end up in the hands of a third party.

7. Encryption systems can be bypassed or may contain backdoors

There are many examples of situations where encryption systems have been bypassed and there are many ways to implement backdoors into encryption

systems[xxxiv]. More recently, following the Snowden/PRISM leaks, it has been revealed that Microsoft worked with the NSA to bypass its own encryption[xxxv], for email, chat and cloud storage[xxxvi]. Although Microsoft has denied such a claim[xxxvii], the simple fact that these encryption systems can be bypassed, and that backdoor access can be given to a third party, should be enough to ring a bell and shed light on the extent of the security and privacy problem globally.

This of course is only the tip of the iceberg. Many other organizations and governments worldwide are involved and new revelations continue to abound. Backdoors may be government-mandated, but they may also be implemented by encryption technology manufacturers and services providers for other reasons, including convenience in recovery and other administrative functions. Other than government access and other accesses knowingly granted by manufacturers and service providers, the primary hazard is that backdoors are also available to hackers[xxxviii].

In cloud environments, because technological environments and service providers may be different and may be located in various geographical locations, it's virtually impossible to confirm the reliability of encryption systems an whether or not they can be bypassed or have backdoors.

8. Local laws may compel someone to decrypt or provide the keys

Contrary to popular belief, key disclosure laws are a reality and vary widely between national jurisdictions[xxxix]. There are numerous examples of such laws being applied[xl], or where an individual or an entity has been forced to provide decryption keys or decrypt the data under its control[xli, xlii].

Some jurisdictions may also force telecommunication companies, internet service providers and storage providers to compromise encryption[xliii] or provide backdoors to their systems[xliv].

Once again, the distributed nature of the Internet, especially the cloud, makes it virtually impossible to confirm that decryption keys will not have to be disclosed at some point or another and end up in the hands of a third party.

9. Sooner or later, encryption will be broken

This is a very controversial subject, but it has been demonstrated over and over again in the past that encryption is not infallible (DES[xlv], SSL [xlvi, xlvii, xlviii], TLS[xlix], PBC[l, li], WC3/XML[lii]). Weaknesses in encryption algorithms are regularly discovered and research is ongoing. Who would have thought that AES-256 had

its own weaknesses[liii, liv, lv], or that it could be cracked in some situations[lvi]?

Not only does technology evolve and processing power increase, but new methods of calculation, including quantum computing, may one day signal more sombre days for encryption[lvii]. In fact, we know that various organizations throughout the world may keep encrypted data for long periods of time, hoping or knowing that someday it will be possible to decrypt it[lviii].

Although breaking the more recent and robust encryption algorithms may be harder to break[lix], it is important to keep in mind that our beliefs are based on the paradigm of our time. When people say that millions of years would be required to break an encryption algorithm, they assume the current state of technology, and knowledge. But who knows what the future will bring? For all we know, any encryption algorithm could be found vulnerable overnight. Relying solely on encryption therefore, to protect sensitive information, is risky and may not be the best idea in the long run.

10. Data encryption has an impact on performance

Depending where and how encryption is implemented may have a noticeable impact on the performance of data transfer, processing and storage[lx]. Furthermore, since encryption occurs in different ways and at several points throughout the computing environment and the communication cycle, performance degradation and technical problems are compounded. Maintaining performance objectives in these scenarios require more powerful equipment or the use of dedicated hardware encryption devices[lxi]. And as we know, especially in the cloud, more devices, more providers and more technology translates into greater vulnerability for your data and more risk.

On the other hand, performance issues and other problems related to user experience with encryption may burden and frustrate users, to the point that they will sometimes bypass or try to bypass these systems when possible[lxii].

11. Encrypted data must be decrypted so that it can be used

One of the main problems with encryption is that it renders your data useless while it is encrypted. Besides storing and moving your encrypted data around, you can't do anything with it. If you want to get any value from your data, it must be decrypted[lxiii].

For example, most healthcare regulations allow data to be stored in the cloud as long as they're secured. The regulations however also require making the data

available for statistical analysis (e.g.: for detecting and tracking epidemics and diseases). However, there's no practical way to perform such analysis without decrypting the data first[lxiv]. So encryption in these cases may not be a viable option.

12. It may be impossible to retrieve encrypted data

Accessing encrypted data is always dependent of the availability of the decryption key and, depending on the implementation, the password or passphrase required to activate this key. Lose any one of them and your data may be lost forever[lxv].

This is true with all types of encryption implementation, but particularly so when disk encryption is used and the disk fails[lxvi]. Not only do you need a backup copy of the data, but you also need a backup copy of the decryption key. It goes without saying therefore that security measures will also have to be deployed to protect this key. Once again, this increases the vulnerability of your data and the risks of a data breach.

13. Restoring encrypted data from backup copies is hazardous

Restoring encrypted data from backups and other storage devices is tricky and fraught with obstacles. Encryption and decryption processes may work fine during normal operations, but it's a different story when time comes to restore data from encrypted backups, or storage devices, especially if they haven't been used for some time.

Backups are the traditional starting point for data protection. Since they involve risks at multiple points (transportation, third party custody, recovery of data, etc.), encryption of backups certainly appear appropriate. It enables safe transport and storage of the data, as long as the passwords and encryption keys are kept separate from the data itself, of course. When time comes to restore data from the backups however, encryption makes things harder, not easier[lxvii].

Retrieving information from encrypted backups requires the implementation of a system and a comprehensive key management process, including testing, that can guaranty data restoration and sustain the test of time. Throughout the process, many problems can occur, including the non availability of the decryption keys, the non availability of the decryption application or its appropriate version, the corruption of the decryption keys, job rotation and technology obsolescence, just to name a few[lxviii].

CONCLUSION

This article demonstrates that encryption is not the miracle cure to security and privacy problems that it is often purported to be.

In this new era of cloud computing, your data is sent all over the place, in different geographical locations and jurisdictions. You cannot prevent your data from crossing national boundaries. Your data is frequently misused, accessed by a large number of people and companies, transferred to subcontractors and surrendered to third parties, without your knowledge or consent. Your data can be accessed by hundreds of individuals and organisations, as part of regular operations, and it is constantly exposed to breaches. In this context, encryption alone is definitely not the answer.

Internet service providers and storage providers are not immune to risk. No matter which security measures they deploy, including encryption, they will never be fully responsible for the damages that may result from a data security or privacy breach. Data protection and privacy laws, on the other hand, are disparate throughout the world and cannot keep up with technological advancements. Encryption alone will not solve information security and privacy problems, let alone liberty, freedom and democracy.

It is time to think out of the box and change the current paradigm.

At VoD2, we are dedicated to reinventing Internet and cloud security using other means than encryption. Our objective is to bring to people and organizations the most innovative, effective and comprehensive information security and privacy solution for data storage in the cloud. You may visit VoD2.com for more information.

What was written 20 years ago in a Wired article is still applicable today:

> *"...Encryption has been vastly oversold as a privacy protector. The biggest threats to our privacy in a digital world come not from what we keep secret but from what we reveal willingly. We lose privacy in a digital world because it becomes cheap and easy to collate and transmit data... Restricting these invasions of privacy is a challenge, but it isn't a job for encryption. Encryption can't protect you from the misuse of data you surrendered willingly..."*[lxix]

[i] Is Encryption Doomed?: http://www.technologyreview.com/news/403031/is-encryption-doomed/
[ii] Who needs encryption?: http://blogs.msdn.com/b/lcris/archive/2006/11/30/who-needs-encryption.aspx
[iii] When Encryption Gets in the Way of Data Availability: http://www.devx.com/blog/encryption-vs.-data-availability.html
[iv] Why Encryption Might Not Stop Data Theft: http://seacliffpartners.com/wordpress/?p=600
[v] Why Encryption Might Not Stop Data Theft: http://seacliffpartners.com/wordpress/?p=600
[vi] In the Cloud, Encryption in Motion + Encryption at Rest = Not Good Enough: http://www.devx.com/blog/in-the-cloud-encryption-in-motion-encryption-at-rest-not-good-enough.html
[vii] Data in Motion: The Other side of the Cloud Encryption Coin: http://cloud.trendmicro.com/data-in-motion-the-other-side-of-the-cloud-encryption-coin/
[viii] Encryption is Not Enough: http://www.techsupportalert.com/content/encryption-not-enough.htm
[ix] Security Pitfalls in Cryptography: http://www.schneier.com/essay-028.html
[x] NIST-certified USB Flash drives with hardware encryption cracked: http://www.h-online.com/security/news/item/NIST-certified-USB-Flash-drives-with-hardware-encryption-cracked-895308.html
[xi] Faulty implementation of cryptographic software: https://mycotopia.net/forums/resist-rebel/68108-~open-discussion-privacy-security-tip-day-~.html
[xii] Security Fail: Apple iOS Password Managers: http://www.informationweek.com/security/encryption/security-fail-apple-ios-password-manager/232602738
[xiii] Encryption in the Cloud: http://wrlapinsky.wordpress.com/2011/02/13/encryption-in-the-cloud/
[xiv] Encryption in the Clouds: http://blog.esds.co.in/encryption-in-the-clouds/
[xv] Porticor - Securing Data in the Cloud: http://www.porticor.com/wp-content/uploads/2012/10/Porticor-White-Paper_Nov_2012.pdf
[xvi] VeriSign Hacked: What We Don't Know Might Hurt Us: http://www.pcworld.com/article/249242/verisign_hacked_what_we_dont_know_might_hurt_us.html,
[xvii] VeriSign admits security breach of corporate network: http://www.computerweekly.com/news/2240114786/Verisign-admits-security-breach-of-corporate-network
[xviii] Key Internet operator VeriSign hit by hackers: http://www.reuters.com/article/2012/02/02/us-hacking-verisign-idUSTRE8110Z820120202
[xix] RSA Warns SecurID Customers After Company Is Hacked: http://www.pcworld.com/article/222522/article.html
[xx] RSA Faces Angry Users After Breach: http://www.nytimes.com/2011/06/08/business/08security.html?pagewanted=all
[xxi] SecurID Customers Advised To Prepare For Worst Case: http://www.informationweek.com/security/attacks/securid-customers-advised-to-prepare-for/229301337
[xxii] Huge Security Breach at Security Firm Symantec No Threat to Consumers, Analyst Says: http://www.foxnews.com/tech/2012/01/06/symantec-source-code-theft-likely-no-threat-to-average-user-analyst-says/
[xxiii] Symantec tells users to stop using pcAnywhere amid security breach: http://betanews.com/2012/01/26/symantec-tells-users-to-stop-using-pcanywhere-amid-security-breach/
[xxiv] Symantec source code breach saga continues: http://nakedsecurity.sophos.com/2012/01/19/symantec-source-code-breach-saga-continues/
[xxv] Web credential authority rebuked for 'poor' security: http://www.theregister.co.uk/2011/11/03/certificate_authority_banished/
[xxvi] Another certificate authority issues dangerous certificates: http://nakedsecurity.sophos.com/2011/11/03/another-certificate-authority-issues-dangerous-certficates/
[xxvii] More CAs Report Breaches, Suspend Issuing SSL Certificates: http://www.eweek.com/print/c/a/Security/More-CAs-Report-Breaches-Suspend-Issuing-SSL-Certificates-479218/
[xxviii] The Problems with Encrypting Data in the Cloud: http://www.devx.com/blog/the-problems-with-encrypting-data-in-the-cloud.html

[xxix] Why Cloud Encryption is a Tough Cloud Security Issue": http://cloudcomputing.sys-con.com/node/2259334
[xxx] Apple holds the master decryption key when it comes to iCloud security, privacy: http://arstechnica.com/apple/2012/04/apple-holds-the-master-key-when-it-comes-to-icloud-security-privacy/
[xxxi] Sony faces setback as hackers release PlayStation 3 decryption keys: http://arstechnica.com/gaming/2012/10/sony-faces-setback-as-hackers-release-playstation-3-decryption-keys/
[xxxii] NSA requests encrypted keys to directly access companies' data: http://www.globalpost.com/dispatch/news/business/technology/130726/nsa-requests-encrypted-keys-directly-access-companies-data
[xxxiii] Feds put heat on Web firms for master encryption keys: http://news.cnet.com/8301-13578_3-57595202-38/feds-put-heat-on-web-firms-for-master-encryption-keys/
[xxxiv] How to 'backdoor' an encryption app: http://blog.cryptographyengineering.com/2013/06/how-to-backdoor-encryption-app.html
[xxxv] Microsoft helped the NSA bypass encryption, new Snowden leak reveals: http://rt.com/usa/microsoft-nsa-snowden-leak-971/
[xxxvi] Microsoft let NSA bypass encryption on mail, chats and cloud storage, says Guardian: http://www.nbcnews.com/technology/microsoft-let-nsa-bypass-encryption-mail-chats-cloud-storage-says-6C10607490
[xxxvii] Snowden Reveals Microsoft PRISM Cooperation: Helped NSA Decrypt Emails, Chats, Skype Conversations: http://www.ibtimes.com/snowden-reveals-microsoft-prism-cooperation-helped-nsa-decrypt-emails-chats-skype-conversations
[xxxviii] Encryption is Not Enough: http://www.techsupportalert.com/content/encryption-not-enough.htm
[xxxix] Key disclosure law: http://en.wikipedia.org/wiki/Key_disclosure_law
[xl] Hand over those decryption keys…or else: http://beris.nl/jb/2012/10/05/hand-over-those-decryption-keys-or-else/
[xli] Judge Rules Americans Can Be Forced to Decrypt Personal Data — What Does That Mean For You?: http://www.popsci.com/technology/article/2012-01/judge-rules-americans-can-be-forced-decrypt-personal-data-%E2%80%94-what-does-mean-you
[xlii] Feds Back Away From Forced Decryption … For Now: http://www.wired.com/threatlevel/2013/08/forced-decryption-legal-battle/
[xliii] PRISM: Here's how the NSA wiretapped the Internet: http://www.zdnet.com/prism-heres-how-the-nsa-wiretapped-the-internet_p2-7000016565/
[xliv] Pure Madness: U.S. Aims to Force Web Services to Compromise Message Encryption: http://stratrisks.com/geostrat/12323
[xlv] U.S. govt.'s encryption standard cracked in record time: http://www.networkworld.com/news/0720des.html
[xlvi] Hackers break SSL encryption used by millions of sites: http://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/
[xlvii] Researchers claim to have broken SSL/TLS encryption: http://www.computerweekly.com/news/2240105674/Researchers-claim-to-have-broken-SSL-TLS-encryption
[xlviii] Online banking encryption broken: http://www.cbc.ca/news/technology/story/2011/09/20/technology-tls-encryption-attack.html
[xlix] Cryptographers Demonstrate New Crack For Common Web Encryption: http://www.forbes.com/sites/andygreenberg/2013/03/13/cryptographers-show-mathematically-crackable-flaws-in-common-web-encryption/
[l] Japanese Researchers Crack Supposedly Hack-Proof Cryptography: http://www.dailytech.com/Japanese+Researchers+Crack+Supposedly+HackProof+Cryptography/article24965.htm
[li] Code crackers break 923-bit encryption record: http://news.cnet.com/8301-1009_3-57457470-83/code-crackers-break-923-bit-encryption-record/
[lii] Researchers crack W3C encryption standard for XML: http://arstechnica.com/business/2011/10/researchers-break-w3c-encryption-standard-for-xml/
[liii] AES encryption is cracked: http://www.theinquirer.net/inquirer/news/2102435/aes-encryption-cracked

[liv] AES proved vulnerable by Microsoft researchers: http://www.computerworld.com/s/article/9219297/AES_proved_vulnerable_by_Microsoft_researchers
[lv] Password Cracking AES-256 DMGs and Epic Self-Pwnage: https://blog.whitehatsec.com/cracking-aes-256-dmgs-and-epic-self-pwnage/#.UdSO4vnNQp8
[lvi] Feds Back Away From Forced Decryption … For Now: http://www.wired.com/threatlevel/2013/08/forced-decryption-legal-battle/
[lvii] The clock is ticking for encryption: http://www.computerworld.com/s/article/354997/The_Clock_Is_Ticking_for_Encryption
[lviii] Leaked NSA Doc Says It Can Collect And Keep Your Encrypted Data As Long As It Takes To Crack It: http://www.forbes.com/sites/andygreenberg/2013/06/20/leaked-nsa-doc-says-it-can-collect-and-keep-your-encrypted-data-as-long-as-it-takes-to-crack-it/
[lix] Is Encryption Doomed?: http://www.technologyreview.com/news/403031/is-encryption-doomed/
[lx] Performance Analysis of Data Encryption Algorithms: http://www.cs.wustl.edu/~jain/cse567-06/ftp/encryption_perf/
[lxi] What you need to know about storage encryption products: http://searchstorage.techtarget.com/What-you-need-to-know-about-storage-encryption-products
[lxii] Solving Enterprise Data Encryption Issues: http://www.examiner.com/article/solving-enterprise-data-encryption-issues
[lxiii] Encryption Is Not the Answer to Security Problems: http://taosecurity.blogspot.ca/2012/09/i-just-read-cyber-fail-why-cant.html
[lxiv] The Problems with Encrypting Data in the Cloud: http://www.devx.com/blog/the-problems-with-encrypting-data-in-the-cloud.html
[lxv] Poor Encryption Key Management Leads to Unrecoverable Data, Survey Finds: http://www.eweek.com/c/a/Security/Poor-Encryption-Key-Management-Leads-to-Unrecoverable-Data-Survey-Finds-673838/
[lxvi] The Problem with Disk Encryption: http://redmondmag.com/articles/2010/02/01/the-problem-with-disk-encryption.aspx
[lxvii] Should we be encrypting backups? It's about the restore, stupid: http://www.theregister.co.uk/2010/06/01/encrypting_backups/
[lxviii] When Encryption Gets in the Way of Data Availability: http://www.devx.com/blog/encryption-vs.-data-availability.html
[lxix] Don't Worry Be Happy: http://www.wired.com/wired/archive/2.06/nsa.clipper.html