

Round Table Report

The role of encryption in cloud computing for data privacy and security

1 April 2015, Brussels

Openforum Academy



Round Table Report
The role of encryption in cloud computing for data privacy and security

Speakers

Jon Crowcroft - Professor of Communications Systems (University of Cambridge), jointly leading the Microsoft Cloud Computing Research Centre

Danny DeCock - PhD researcher at KU Leuven

Moderator: Graham Taylor, CEO of OpenForum Europe

Rapporteur: Diana Cocoru, Senior Policy Analyst at OpenForum Europe

Credits:

Photo by FutUndBeidl is licensed under [CC BY 4.0](#)

White Paper "The role of encryption in cloud computing for data privacy and security" is attributed to OpenForum Europe under license [CC BY SA 4.0](#)

Disclaimer:

This report was prepared by our rapporteur, Diana Cocoru, for OpenForum Academy (OFA). The summaries of the speakers' introductions and following discussions presented in this report are based on the rapporteur's notes and they are not in any way binding or necessarily complete. All effort has been given to reflect and convey objectively the essence of the speakers' presentations and the discussion.

The views expressed in the report do not necessarily reflect those of the rapporteur or OFA. Neither the rapporteur, nor OFA should be held accountable for any claimed deviation from the original speeches.

OpenForum Academy gratefully acknowledges IBM's and Oracle's sponsoring of the event. OFA welcomes financial support for its events, but always maintains independence of the discussion itself and the follow up White Paper.

Introduction

A consensus is growing among IT security experts that security must focus on the data itself, rather than on its physical location or the infrastructure. This helps ensure that data remains safe both at rest and in transit, even if physical access to the device holding the data is gained.

Today, encryption is considered one of the most effective data protection controls available, when correlated with good authentication, authorisation and auditing. When using encryption, data is encoded, using certain algorithms, with either symmetric or asymmetric cryptography. For data that is encrypted, access is regulated through the controlled distribution of decryption keys.

While some consider that encryption is the solution to all problems, because it solves the issue of unlawful or unauthorised access, others consider that the use of encryption impedes national surveillance agencies from getting access to data, in order to prevent security breaches, terrorist attacks and the like. Added to this, encryption in the context of cloud makes the issue even more complex, with the need to separate the data storage from the key management, and the risk concerning the integrity of the information. Integrity, the protection of (and validation of access to) data are much more important when the client depends on a cloud service provider than when the data is stored in a local data center. Moreover, as far as cloud cryptography is concerned, challenges do not always lie in technology, yet sometimes the entire economic ecosystem of cloud computing is put at risk by requiring unsuitable technological solutions, based on threats that are not always grounded or proved.

To discuss all these issues and to present the latest arguments and some of the current research regarding encryption and cloud computing, OpenForum Academy invited two speakers: Danny DeCock, PhD researcher at KU Leuven, and Jon Crowcroft, Professor of Communications Systems at the University of Cambridge, who also jointly leads the Microsoft Cloud Computing Research Centre.

The discussion tackled the following questions and more:

- Which is the main driving force of encryption: compliance with data protection regulation, protection of customer/user data from unauthorised access, protection from government surveillance, or deterring theft?
- How to make sure that when moving encrypted data into and out of the cloud, the client also benefits from the interoperability of keying methods, without being limited by the provider?
- Which policy actions are needed in order to ensure that encryption methods are correctly matched with the scenarios envisioned?

Various approaches to encryption and practical solutions

The first question to ask when analysing the role of encryption is what are the threats that it tries to respond to. There are several motivations behind the decision to encrypt data: protection from government surveillance, protection of user data from unauthorised access or protection against theft. The role played by these potential scenarios depends on the type of data stored and its value for the ones who are searching to get this data. For instance, if you are a business, the NSA might not be interested to access your data, because it does not correspond to the type of data that they are searching for.

Professor Crowcroft underlined that a much more frequent threat than the risk of government surveillance is the accidental disclosure of private information, e.g. credit card information. Sometimes this is due to operational practice (hacking), but more often it is caused by security flaws in software (e.g. failure to use SSL-encrypted connections) or bad processes which open the door for human errors. Moreover, although this practice has largely stopped nowadays, data is sometimes moved between data centers of the same provider in unencrypted form.

Depending on the threat model that is being faced, information may need to be protected in a different way. For instance, if a company fears an internal threat, e.g. the risk of data being stolen by

Round Table Report
The role of encryption in cloud computing for data privacy and security

one of its employees, then it makes sense to store all the data in an encrypted manner. But if the company trusts its employees and encrypting data could trigger consequences (legal and other) that might result in bankruptcy of the business, then the company might just as well decide not to encrypt its data. Professor DeCock pointed out that one needs to consider the application in which the data is going to be used in the cloud system. Depending on the environment, the decision might be to not encrypt data, in case there is a possibility of being sued if decryption cannot be achieved easily. He took the example of a hospital which risks being sued for not being able to decrypt a patient's file when a life-critical decision needs to be made urgently. Therefore, sometimes it really makes sense to choose not to encrypt data.

Because encryption shifts the burden of what needs to be protected from the data itself (very large) to the keys (very small), encryption makes it all about access control and key management. Professor DeCock expressed his preference for protecting the access to data with strong authentication, using hardware devices that prove the identity of the person who requests access to the information, rather than depending on the technological mechanisms of encryption. He pointed out that although he works in the field of cryptography, he is not always using encryption, because encryption should be used only when necessary.

Encryption becomes very important when data is stored remotely. Even though the relevant contract might have provisions that oblige the data center operator to obey all the conditions requested by the client, in reality the best way for the client to trust its provider is to ensure that the provider is not able to access the data. When data is stored in the cloud, there is no certainty that the cloud operator would not modify the information. Therefore the integrity of the information and its protection is much more important when there is a dependency on a cloud service provider than when all the data is stored on premises.

The issue of interoperability was also raised. For instance, whenever research conducted in a university is stored in databases, in the case that the researchers graduate and leave the university, their findings need to continue to be accessible, in a usable and accessible format, for the next person to be able to take that research further. Another interoperability issue arises when end users are not able to use encryption keys from one device to the other, because in the current stage it is difficult to implement cryptography across devices. The question which arises is whether cloud can be seen as a solution to this issue. While Professor Crowcroft was able to point to a project which manages keys across devices in an effort to solve this issue, Danny DeCock underlined that because of all the different client applications which are being used, which do not necessarily allow sharing of settings, a better solution would be to use a container with standardised APIs. In this case, the

Round Table Report
The role of encryption in cloud computing for data privacy and security

implementation could depend on a cloud provider so that the user can access it from wherever it is needed. His remark was that although the technology could allow this solution, there is no incentive to close the existing gap and provide such a solution.

There are a number of different initiatives which seek to respond to the different challenges presented above, in different ways. For instance, in order to avoid the risk of data stored in the cloud being stolen, or surveillance authorities obtaining data directly from the cloud provider, currently efforts are being invested in building a decentralised cloud computing platform. Professor Crowcroft made the remark that it seems quite feasible to actually source all the data from the device located at home (i.e. peer-to-peer cloud), in a cloud system built on a device which costs 50 EUR and which gives a variety of properties and services. This would use less energy, because a peer-to-peer cloud uses the energy only of computers in homes, rather than having big data centers as well, and also because the mean path length between peers is half (i.e. it does not have to go up to cloud data center and back down to other user). For the same reason, it also has lower latency. This model also offers the needed privacy, because no one else can access the data located on that device, unless specific access is granted by the client, by its own choice. When such a scenario is presented, in the case of an official request to provide data, the cloud provider literally cannot honour the demand because the requested data is on a device kept in the client's house, car etc. This business model is actually perceived as a credible threat by some companies (e.g. Amazon, Microsoft Azure), due to the benefits that it offers to the client, because it replaces the need for the centralised data centers, and removes the need to have a payment system (whether money or through advertising and analytics revenue), since it just relies on end users equipment only.

In order to avoid the risk of managing unencrypted data for whatever purposes, homomorphic encryption can be used. Some companies have developed and patented specific implementation solutions for this type of encryption. Through this form of cryptography, the data is processed while remaining encrypted. The disadvantage underlined by Professor Crowcroft is that (currently) the processing is way too slow to be practical. Once this challenge is tackled, homomorphic encryption could become a game changer, because it will enable analytics to be carried out on data, without any ability to identify the source of the data, thus respecting privacy rules. However, no one is capable of foreseeing when – or even if – this method will become feasible (or affordable). Mr DeCock added that besides the disadvantage of it being too slow, another aspect is that data grows gigantically, which tends to make this method unusable in real life systems. Homomorphic encryption systems are very useful in practice only for voting systems, because they make it easy to calculate the results, but he pointed out that for real analysis applications, the method is completely unusable.

Round Table Report
The role of encryption in cloud computing for data privacy and security

Because encryption moves the risk from the management of data to the management of keys, another issue to consider is the situation when keys are damaged or missing, thus preventing the encrypted data from being accessed. To avoid the risk of no longer having access to keys which decrypt the data, what can be used is a secure encrypted data container, which can be referred to (using pointers) whenever necessary. Mr DeCock pointed to a European project which involved healthcare providers, employment institutes, universities and potential employment markets, in which all information about certain persons (patients, employees etc.) was exchanged through an encrypted data container, with dedicated keys. In this setup, the keys were used only for confidentiality purposes. After proper authorisation and proof of possession of the correct mandate, access was granted to the decryption keys. With this setup, even if keys are lost, access to the information is maintained because the secure information container is self contained, with references to the key material, and also indicates the party which could help in case something goes wrong. Moreover, it becomes irrelevant which party (the government, employer etc.) is holding access to the escrow functionality, because it needs to be controlled properly, through legal and policy means that have to be enforced.

At the European level, the Commission is working to see if certain communications should be included in the scope of the European cloud framework and whether encryption should be at least offered as part of the service. If this is adopted and implemented, if a cloud provider wants to be listed as a secure electronic communication server, it should also offer certain interoperability features with respect to encryption methods. It has been suggested that buttons should even be included on websites, to allow citizens to turn encryption on or off, in an attempt to make it easy for citizens to use encryption methods without extensive IT knowledge.

To address the problem of interoperability and dynamic evolution of encryption algorithms, which can impede future access to versions of files which used old algorithms, people are calling for an open library of cryptographic methods that have been used to encrypt those files. Openness makes it easier to see the algorithms and ensure the methods are secure. Openness *per se* does not guarantee security, unless the code is actually reviewed in order to trust it. Although there was an agreement between the speakers that there are some cryptographic algorithms which are not – nor should be – public, in general they agreed that encryption algorithms should belong to an open library, in order in the future to be able to look back and track cryptographic methods which were used in the past and to allow data to be decrypted depending on the needs.

Participants to the discussion also pointed out that it seems easier to speak about cryptography than

to explain what the threat models are. Often, when talking about cloud cryptography, people are looking at challenges that do not always lie in the technology itself. It is important to acknowledge that it is not possible to solve a problem with cryptography, if it is not a cryptography problem to start with. Europe is currently dealing with legal and policy issues which are sometimes tugged under cryptography. For instance, the biggest failure in the Snowden case, as underlined by Professor Crowcroft, is that one individual had access to, and was able to download copies of as many as 2 million documents, without anyone apparently being able to notice it. He made the point that if someone did this at the MIT, the person would have been caught immediately. Therefore this situation has nothing to do with the complexity of cryptography, it is just evidence of bad operating practice, i.e. the lack of certified security processes within the specific data handling facility or network.

Up to now, surveillance authorities have not been able to produce credible figures quantifying the value of weakening cryptography for the cloud. Although Rob Wainwright (Europol Director) considers encryption as a blocker to the identification of security threats, surveillance authorities are more and more requested to present instances of cases which they could not solve because of encryption. Professor Crowcroft pointed to the fact that authorities failed to capture the post-marathon bombers (Boston, 2013) even though the names of those responsible of the attack were already on a “watch list”. In order to become convincing, surveillance authorities need to provide a credible threat, together with figures quantifying the value of weakening cryptographic systems in order to spot and stop security attacks. Otherwise, by requesting access to encrypted data or weakening cryptographic systems, when in reality attacks could have been identified and perhaps prevented even without access to the encrypted data, and justifying this with the need to identify security threats, undermines the entire economic ecosystem of the cloud and the internet, an ecosystem that allows to cut huge amounts of costs of overheads.

Conclusions

Policy makers, businesses and users alike are confronted with different threat models that require different security solutions. Encryption is only part of the solution, as long as the right cryptographic method is matched with the scenario at hand, and encryption is used together with proper authentication and audit methods. There is no one-size-fits-all solution and therefore a differentiated approach is needed.

Round Table Report
The role of encryption in cloud computing for data privacy and security

Member States should do more to protect confidentiality and privacy of communication of their citizens. In order to contribute to the clarity of security methods, governments should specify what needs to be achieved for each of the various categories of information exchange per policy sector (e.g. health, finance, culture etc.), and should be specific about what sort of information they are referring to. When governments regulate the mechanisms that need to be used, they should also specify that data still needs to remain accessible and - if it is no longer accessible -, that it needs to be converted into something which remains accessible over time. Moreover, it should not be overlooked that at national and international level, there are reasonable exceptions where governments are entitled to ask for the keys to decrypt data (e.g. Ebola outbreak cases or money laundering cases). The list of sectors where such legal exceptions are reasonable should be clarified.

Although data in transit is being taken care of already, the problem remains that there are no incentives for service providers which are not government-like to take specific actions to ensure the integrity of data in transit and data at rest. Currently, the commercial service providers allow themselves to act according to their business interest, as long as they are not being sued. These providers should be encouraged to make sure that they are obeying the same rules, and policy-makers should make sure that incentives are created across the board for service providers to implement the services rightfully and lawfully.

The discussion concluded with the idea that policy-makers need to strike the right balance between security and privacy. Moreover, transparency and education also have an important role to play when it comes to encryption in cloud computing. Transparency is essential in order to understand what security method is being used, what governments are allowed to do and also what citizens are entitled to. Transparency also allows the legitimacy of those using the security methods to be checked. Education, on the other hand, allows people better to understand that laws exist to protect their privacy and enables stakeholders to apply the best security method, by understanding the benefits of each security solution in relation to specific threat models.

Speakers' Biographies



Jon Crowcroft graduated in Physics from Trinity College, University of Cambridge in 1979, gained an MSc in Computing in 1981 and PhD in 1993, both from UCL. He is a Fellow the Royal Society, a Fellow of the ACM, a Fellow of the British Computer Society, a Fellow of the IET and the Royal Academy of Engineering and a Fellow of the IEEE. He has worked in the area of Internet support for multimedia communications for over 30 years. Three main topics of interest have been scalable multicast routing, practical approaches to traffic management, and the design of deployable end-to-end protocols. Current active research areas are Opportunistic Communications, Social Networks, and techniques and algorithms to scale infrastructure-free mobile systems.



Danny De Cock is an expert in computer security and industrial cryptography applications, currently researching as a post-doc applied cryptography at the KU Leuven in Belgium. He was the coordinator of a study for the four Belgian governments to lay out the security architecture and functionality of the electronic voting system for Belgian elections. Danny is also involved with different identity management projects to increase Belgian eGovernment efficiency on the regional and federal level, and was in charge of the Modinis-IDM study (<http://godot.be/modinis>) that was organized by the European Commission to build on expertise and initiatives in the EU Member States to progress towards a coherent approach in electronic identity management in eGovernment in the European Union.