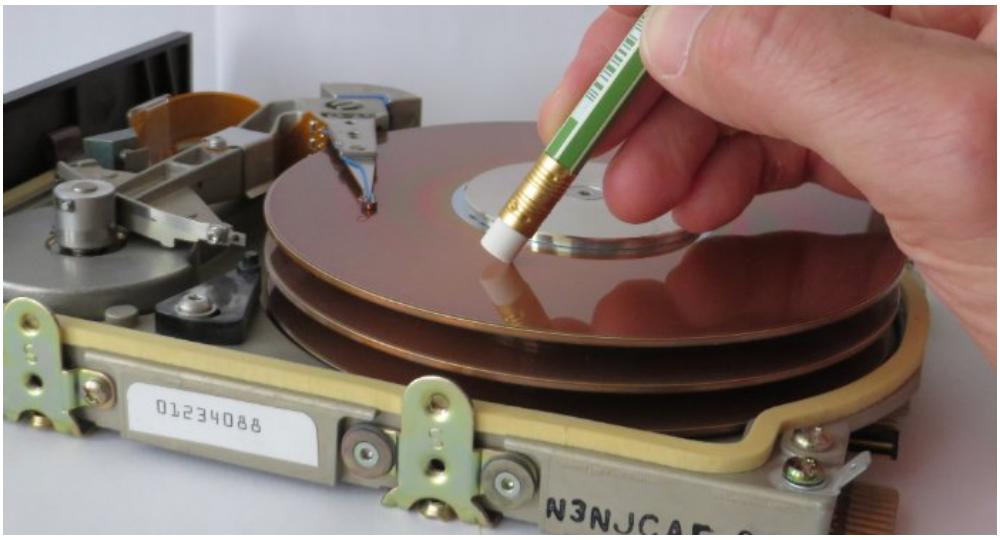

Photo Credit: Christian Cachin

IBM’s Christian Cachin Talks Cryptography for the Cloud

Published on April 27, 2015

Chris Sciacca | Follow
Manager, Communications, EMEA, IBM Research

SUPERCLOUD, ESCUDO-CLOUD and WITDOM are not the names of comic book superheroes, but what they hope to achieve is equally as super — securing data stored in the cloud.

These three EU HORIZON2020 projects recently kicked off, and one IBM cryptographer happens to be involved in all three — Dr. Christian Cachin, who is also president of the International Association for Cryptologic Research.

I recently sat down with Christian to hear about the projects and the challenges which lie ahead.

Q. What is the grand vision for cloud cryptography?
Christian Cachin (CC): We want to make processing data in the cloud more secure and more reliable for users. While most people think of the cloud as a giant hard disk in the sky, you can actually do advanced analytics and processing in the cloud, as well. Clearly any data in the could needs to be secure, so we want to apply cryptographic protection to make sure that your data does not leak to parties that shouldn't have access to it.

Q. Can you discuss the three new EU projects which have recently been awarded?

CC: Sure, SUPERCLOUD is based on a cloud-of-clouds concept for preventing vendor lock-in and for enhanced resilience. It picks up from where our previous project on trustworthy clouds, called TClouds for short, has brought us. In SUPERCLOUD we will focus on user-centric management of security and dependability in a clouds of clouds, together with partners from the telecom and medical industries as well as academia. We will build end-to-end security into distributed storage platforms and provide self-managed security services to users.

ESCUDO-CLOUD stands for Enforceable Security in the Cloud to Uphold Data Ownership. "Escudo" is Portuguese for "shield." Its goal is to give back to users the control over their data in the cloud. Our enforceable security techniques rely on wrapping the data cryptographically, to provide a layer of protection against the prying eyes of whomever may get improper access to it. This moves the trust boundary to the client side, outside of the cloud.

And finally, WITDOM aims to enhance privacy and security for personal data in the cloud. It's actually short for for empoWering prIvacy and securiTy in non-trusteD envirOnMents. It will enable secure sharing and processing of sensitive health data such as genetic information and build methods to protect financial data outsourced to cloud services. Cryptography forms the basis for the privacy-enhancing technologies that will be used. We have legal experts on board here as well, who will assess the technical methods from their perspective.

Q. What is the biggest challenge?

CC: Actually, there are many fascinating challenges. Most importantly, we have to protect the cloud from its users. Think about this, as a cloud provider you are giving total strangers access to your infrastructure and as with IBM Softlayer, clients can get access down to the bare metal of the servers. But what if some nefarious user sets up an account and tries to steal data or plant viruses in your system? It's like giving a stranger the keys to

strong cryptography.

In addition, many servers in the cloud are shared across multiple tenants. For example, as a cloud provider you might suddenly have data from competitors on the same machine. And as a client you don't want anyone else to see your data. So we help address this with a rules and policies based system to prevent these types of incidents.

On the other side, we have the clients. They are concerned about their precious data. They want to limit their exposure as much as possible and reveal as little as is needed for processing the data for a desired outcome. Today, they already have control of which data centre their data is stored in. For example, a German bank can't store its client data in a cloud outside of the EU. But if clients want to enable certain kinds of analytics that do not need the full data set, then the data can be masked cryptographically and only the relevant features are revealed.

Another challenge is trusting the data. How do I know what I am receiving from the cloud is what my friend or collaborator has posted there, that it has not been altered by spyware or subverted by a virus? So we need to detect any violations that may have occurred in the cloud for users who, for example, may be collaborating in the cloud on a joint project. How can the data integrity be verified? We are building systems to address this such as our verification of integrity and consistency of cloud object storage tool (check it out at SYSTOR 2015 at the end of May 2015).

Finally, we are also embracing key management in the cloud. Think of it as keys-as-a-service. Apart from providing enterprise cloud customers with strong protection for their cryptographic keys, this has also a secondary use in ensuring the proper deletion of files. We all know that traces of data remain even when we empty the virtual trash bin, but this isn't acceptable for highly sensitive or personal data. Cloud providers need to offer this assurance and guarantee it - we call this novel feature secure deletion.

We are developing software to address this, which is analogous to smashing a hard disk in a million pieces with a hammer, except that it will be done by destroying an encryption key, alone. The software will also have polices to know if something shouldn't be deleted, such as corporate financial records when an employee leaves the company, which may be needed for audits.

So you can see we have our work cut out for us. Thankfully we have a few years to tackle these challenges.

Q. The cloud market is a multi-billion industry already, don't these technologies exist?

CC: Yes and no. The EU is funding this research to not only help cloud providers, developers and users to understand it better, but also to make it open and sharable. Everything developed in these three projects is funded with public money, so we will publish our results and make most of it available as open source.

So, we are planning for the future to enable more types of businesses to trust and rely on the cloud for any workload.

Tagged in: european union, cloud security

Chris Sciacca
Manager, Communications, EMEA, IBM Research
8 articles

Follow

0 comments

Don't miss more articles by Chris Sciacca

Pathologists Look Forward to a Future with Deep Learning and Neural Networks
Chris Sciacca on LinkedIn

Hacking anti-malarial drug resistance
Chris Sciacca on LinkedIn

Does Your Nanowire have a Fever? A New invention can find out.
Chris Sciacca on LinkedIn