PHYS.ORG

Microsoft research project reveals new method for keeping data private

May 19 2015, by Allison Linn

Microsoft researchers have created a new system that keeps data stored in the cloud safe from prying eyes or malicious players even when it is being accessed to make calculations.

The new research project, released Monday at the IEEE Symposium on Security and Privacy, adds an extra layer of security for companies that are charged with safeguarding very sensitive information, such as financial data or personal records, and also regularly need to use that data to make calculations or conduct other transactions.

The new technology is called Verifiable Confidential Cloud Computing, or VC3, and it works like this:

Let's say a financial services company wants to access a number of clients' personal financial records to make a complex series of calculations in the cloud. That data is stored in a sort of lockbox that can be accessed only within secure hardware managed by VC3.

To make the calculations, the client's data is loaded into the secure hardware in the cloud, where the data is decrypted, processed and re-encrypted. No one else – including the people who work at the company running the cloud-based service – can see or access the data.

That ensures that the data is secure even if the provider has a bad actor in its own ranks, or if someone else has managed to gain access to the provider's system. It also guarantees that no one else could get in and manipulate the results of the calculations, saving the company and its clients from any possibility of financial damage.

"The cloud provider cannot see the data or the code that the customers are using for the analysis," said Manuel Costa, a principal researcher with Microsoft Research Cambridge in the United Kingdom, who was one of the authors of the paper released Monday.

Once the transactions and calculations are complete, the data is again encrypted and moved back across the wire to the secure hardware on which it usually is stored.

The research project is just one instance of a class of work Microsoft is pursuing to ensure it is keeping its customers' data private and safe in the face of growing and complex electronic security and privacy threats.

Sriram Rajamani, the assistant managing director of Microsoft Research India, said one key to helping customers feel more comfortable with cloud-based systems is to ensure that they have the same or better safeguards as compared to on-premises server systems.

"We are investigating ways by which we can tell the customer, 'Even though you move your data to the cloud, you are still in control,'" said Rajamani, who also works on security and privacy issues.

The IEEE conference is running through midweek in San Jose, Calif. In addition to presenting VC3, Microsoft researchers are presenting a number of papers on other elements of security and privacy.

They include:

- A messy state of the union: Taming the composite state machine of TLS: Microsoft researchers collaborated with researchers from the French research institute INRIA, at the MSR-INRIA Joint Centre, along the Spanish research institute IMDEA to bulk up the security of "https" browsers. The researchers found and fixed certain existing vulnerabilities and developed a system for ensuring that the code within the Transport Layer Security protocol is more secure.

- Geppetto: Versatile verifiable computation: Microsoft researchers developed a system for verifying the outcome of computations when they are outsourced to powerful but untrusted cloud computers.
- Controlled-Channel Attacks: Deterministic side channels for untrusted operating systems: Microsoft researchers collaborated with a researcher from The University of Texas at Austin to uncover a new side-channel attack. The side channel may leak sensitive information—such as text documents or images—even if the user is relying on a hypervisor or trusted hardware to protect applications from an operating system that may be under the control of an untrusted cloud provider or that may have been compromised by a virus.
- SurroundWeb: Mitigating privacy concerns in a 3D web browser: A group of Microsoft researchers and a researcher from the University of Massachusetts have developed a 3D browser that allows for immersive experiences while also tackling security and privacy concerns.
- Post-quantum key exchange for the TLS protocol from the ring learning with errors problem: We don't have a fully functional quantum computer yet, but researchers from Microsoft, NXP Semiconductors and Queensland University of Technology are already working on a system for securing the Internet if one is built.
- Securing multiparty online services via certification of symbolic transactions: Researchers at Microsoft collaborated with a Ph.D. student intern from Carnegie Mellon University to develop a

formal verification approach that secures real-world implementations of online services, such as single-sign on systems and third-party payment applications.

Provided by Microsoft

Citation: Microsoft research project reveals new method for keeping data private (2015, May 19) retrieved 10 April 2024 from
https://phys.org/news/2015-05-microsoft-reveals-method-private.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.