On Information Flow Control and Audit for Demonstrable Compliance in the Cloud

Thomas Pasquier, Jatinder Singh and Jean Bacon
University of Cambridge

ABSTRACT

There is pressure for more and better control over personal data in cloud environments. Cloud tenants are increasingly burdened with data management obligations [3], and therefore require assurance of proper data handling throughout the whole-system. We believe a simple technical mechanism can contribute to such guarantees.

Decentralised Information Flow Control (DIFC) is a data-centric mandatory access control scheme that guarantees non-interference across security contexts, based on lattices defined by secrecy and integrity properties. Every data flow is continuously monitored to guarantee the enforcement of (decentrally) specified policies. We demonstrated that DIFC can constrain data flows throughout an entire cloud platform [2]. A simple DIFC constraint confines the flow of data within a security context. Simple constraints can guarantee complex workflow, for example to ensure that data is anonymised before crossing security contexts for disclosure to third parties. We considered the enforcement of some cloud legal requirements [3].

We showed that information captured during DIFC enforcement allows the generation of a provenance-like directed graph representing whole-system data exchange [1]. This coupling of policy enforcement with the capture of audit data allows system "noise" to be removed, so that only the information relevant to the policies in place is recorded. These graphs can be queried to reveal whether system behaviour accords with particular data management obligations. For instance, from data gathered at run-time, we show it can be ascertained that there is no path in which personal data was transferred to another tenant without being anonymised [1].

BODY

Complex policy can be built upon simple primitives enforced on every data flow. Enforcement data can be captured to demonstrate compliance.

REFERENCES

[1] T. Pasquier, J. Singh, J. Bacon, and D. Eyers. Information Flow Audit for PaaS clouds. In *International Conference on Cloud Engineering (IC2E)*. IEEE, 2016.

[2] T. Pasquier, J. Singh, D. Eyers, and J. Bacon. CamFlow: Managed Data-Sharing for Cloud Services. *IEEE Transactions on Cloud Computing*, 2015.

[3] J. Singh, J. Powles, T. Pasquier, and J. Bacon. Data flow management and compliance in cloud computing. *Cloud Computing, IEEE*, 2(4):24–32, July 2015.

Volume 4 of Tiny Transactions on Computer Science