The Trust-to-Trust Model of Cloud Services

Alissa Cooper
Cullen Jennings

Cisco Systems

January 15, 2014

The recent revelations about pervasive surveillance have raised questions about whether businesses and individuals can continue to rely on cloud services to store and manage their data. For businesses in particular, the last several years have seen increased adoption of cloud-based services for everything from file-sharing to real-time communications to office productivity applications [VZES], all of which move sensitive corporate information from the enterprise premises to remote infrastructure managed by cloud providers. The revelations concerning NSA and GCHQ fiber taps, tapping of data center networks, decryption of encrypted traffic, and man-in-the-middle attacks [PervasiveProblem] have left businesses to wonder whether they should continue to entrust their sensitive corporate data and communications to third-party cloud companies. The revelations have likewise spurred policymakers to seek mechanisms to protect their national interests against foreign intelligence agency snooping.

One of the proposed responses to the revelations suggests that cloud companies should store the data of a particular nation or region's citizens and businesses within the geographic boundaries of that nation or region [Scatturo][StepBack]Patriot]. This is not a long-term solution for sustaining trustworthy cloud services. Part of the mission of most foreign intelligence agencies is to collect information from abroad; relocating cloud storage and processing to a particular country does not prevent these foreign agencies from attempting to tap into or exploit vulnerabilities in that country's networks or services. While nation- or region-based cloud services may be less subject to lawful intercept and data requests from foreign powers, it is not targeted lawful requests that have been making news, but the surreptitious bulk collection and exploitation of communications. Furthermore, while the NSA and GCHQ have been identified as the purveyors of pervasive surveillance, nation-state actors in the very same jurisdictions where national cloud service mandates are being suggested may well be capable of carrying out similar attacks, now or in the future. Businesses concerned that their corporate data is traversing networks and infrastructure that have been made vulnerable by intelligence agency activities should not expect that re-locating their data to different countries will make it any safer in the long term.

Nation- or region-limited cloud services are also difficult to square with the increasingly transnational and global nature of business. When business associates in different countries have a video conference, share files, or collaborate on a document, where will their data reside? What happens when those associates both reside in countries that prohibit cloud data from being stored abroad?

Instead of trying to re-locate cloud infrastructure to avoid nation-state surveillance, enterprise cloud services providers should press forward with solutions that businesses can trust regardless of the jurisdiction in which the data resides or the networks that it crosses. This is the only realistic path forward for transnational businesses to continue to sustain the efficiency, productivity, and cost benefits of cloud services without the risk that corporate communications and data are being surveilled in bulk.

Fortunately, enterprise cloud services can leverage the trust boundaries that enterprises already create to provide services that exploit the efficiency and scale of the cloud while limiting the exposure of enterprise data on the network and in the cloud. As outlined in [SecureRAI], enterprise cloud services can leverage existing enterprise identity infrastructure to allow encrypted communications and content destined for the cloud to be decryptable only by the enterprise or entities authorized by the enterprise. Using this approach, employees trust the private keys they receive from their employers' identity providers, and users within different enterprises can authenticate each other using auditable certificate authorities. Communications or content between two employees are encrypted by each client using the public keys of both users and are stored in the cloud. In this way, the data is encrypted end-to-end and the cloud service provider can manage access and updates to it, but cannot decrypt it. Only the enterprises have decryption capability.

This model provides several salient defenses against pervasive surveillance. First, it maintains the benefits of centralized data storage and processing while decentralizing data access. Cloud service providers would no longer be the targets of unauthorized bulk collection or exploitation because the data they hold is not useful without access to the decryption keys (or some means of undermining the encryption scheme, which is still likely costlier for the party seeking the data than obtaining bulk access to data and keys when stored in a single cloud location).

Second, this model pushes decisions about granting authorized access to enterprise data to their rightful place: the enterprise. By controlling its own identity provider, the enterprise is in control of deciding whether anyone other than the parties involved in a communication – IT departments, law enforcement agents, or anyone else – is granted access to it. This could be considered as a spin on the "trust-to-trust" version of the end-to-end argument [T2T], which envisions network functions being pushed to entities to which endpoints have delegated their trust to implement those functions. In an enterprise environment, the enterprise itself is the natural arbiter of these data access decisions – not the cloud provider.

This trust-to-trust model is also consistent with the notion that where intercept or third-party access capabilities are supported, they should be implemented as "front doors" – in intentional, documented ways – rather than as covert "back doors" that may create risks of exploitation. Because decisions about granting third party access have to be made by enterprises themselves, cloud service providers must explicitly decide to support third-party access capabilities and must provide documentation about how to use those capabilities to their customers. Cloud service providers may or may not support these capabilities, but either way the model of decentralized access makes the idea of planting (or compelling the cloud provider to plant) back doors within the cloud provider's own infrastructure much less attractive.

Finally, the trust-to-trust model renders the physical location of cloud storage less important from a privacy perspective. Because the cloud service provider cannot access its customers' data, the capabilities of local intelligence agencies and the laws controlling government access to data are not material to the question of whether data stored in the cloud can be accessed by third parties.

The trust-to-trust model is just one example of how enterprise cloud services providers can defend against pervasive surveillance through technological means and it has its limitations. For example, metadata about communications – who is calling whom, at the enterprise or user level – may still be visible to the cloud provider. Nonetheless, widespread deployment of the trust-to-trust model would represent a significant improvement in defenses against pervasive surveillance. Ensuring that businesses worldwide can continue to reap the benefits of borderless cloud services, unencumbered by national or regional cloud storage requirements, requires that cloud providers continue to seek these kinds of novel security solutions that let cloud providers focus on delivering the performance, resiliency, and efficiency gains characteristic of the cloud while empowering enterprises to be in control of their own data.

References

[Patriot] L. Munn, "British Columbia's Privacy Laws Amended In Response to the USA Patriot Act," 2004, http://www.cwilson.com/services/18-resource-centre/190-british-columbias-privacy-laws-amended-in-response-to-the-usa-patriot-act.html

[PervasiveProblem] R. Barnes et al., "Pervasive Attack: A Threat Model and Problem Statement," Jan. 2014, http://tools.ietf.org/html/draft-barnes-pervasive-problem-00.

[Quest] M. Scatturo, "The Quest to Build an NSA-Proof Cloud," Nov. 2013, http://www.theatlantic.com/international/archive/2013/11/the-quest-to-build-an-nsa-proof-cloud/281704/.

[SecureRAI] C. Jennings, "Building Trustable Cloud Systems," Oct. 2013, https://www.ietf.org/id/draft-jennings-perpass-secure-rai-cloud-00.pdf.

[StepBack] K. Hustad, "In light of NSA spying, Brazil may take a step back from World Wide Web," Nov. 2013, http://www.csmonitor.com/Innovation/2013/1112/In-light-of-NSA-spying-Brazil-may-take-a-step-back-from-World-Wide-Web.

[T2T] D. Clark and M. Blumenthal, "The end-to-end argument and application design: the role of trust," Aug. 2007, http://groups.csail.mit.edu/ana/Publications/PubPDFs/End%202%20end%20argument%20and%20application%20design%20final%20TPRC2007.pdf.

[VZES] Verizon Enterprise Cloud Services, "2013 State of the Enterprise Cloud Report," Aug. 2013, http://www.slideshare.net/VerizonEnterpriseSolutions/2013-state-of-the-enterprise-cloud-report.