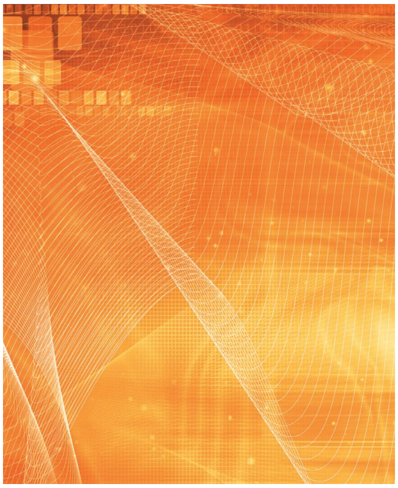
2013-06

Empowering users through secure on-demand data provisioning

Michael, James Bret

IEEE

J.B. Michael, "Empowering users through secure on-demand data provisioning,"
Computer, (June 2013, pp. 84-85.
http://hdl.handle.net/10945/56531



Empowering Users through Secure On-Demand Data Provisioning

James Bret Michael, *Naval Postgraduate School*

A virtualized on-demand infrastructure coupled with multidimensional encryption lets users retain control over their stored data and securely access it from anywhere.

Today, users of cloud-based data storage services trust that service providers will adequately protect their data and privacy. However, most users are unaware of service providers' security policies and enforcement mechanisms. In addition, users often don't know where their data is stored or who's managing it, such as when their smartphone apps and service providers' back-end systems push and pull data between the mobile device and the cloud.

Steven M. Bellovin argues that two key questions to ask regarding cloud computing security are "What are you trying to protect against whom?" and "Secure compared to which alternatives?" ("Clouds from Both Sides," *IEEE Security & Privacy*, May/June 2011, p. 88).

In response to the first question, the goal of cloud computing security is to protect the confidentiality, integrity, and availability of a user's data from both service providers and other cloud storage service users. For example, one user shouldn't be able to determine the contents of another user's online files by exploiting vulnerabilities arising from a provider's use of data deduplication techniques (D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Side Channels in Cloud Services: Deduplication in Cloud Storage," *IEEE Security & Privacy*, Nov./Dec. 2010, pp. 40-47).

Regarding the second question, I believe the answer should be given in terms of user-oriented versus provider-oriented control of online data.

USER-ORIENTED CONTROL OF ONLINE DATA

The idea of giving users control over their data isn't new.

In 1985, the US Department of Defense's *Trusted Computer System Evaluation Criteria* (DoD 5200.28-STD) formally defined *discretionary access control*, providing a standard for user-oriented access control in modern operating and database management systems.

More recently, researchers have explored user-oriented control over data stored and managed via cloud services. For example, a proposed *privacy as a service* consists of "user-configurable software protection and data privacy categorization mechanisms," user-held data encryption keys, and "a privacy feedback process which informs users of the different privacy operations applied on their data" by the service provider (W. Itani, A. Kayssi, and A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," *Proc. 8th IEEE Int'l Conf. Dependable, Autonomic and Secure Computing* [DASC 09], IEEE CS, 2009, pp. 711-716).

At Unified Data Solutions, we're also investigating ways to provide users with more control over their data's security and, ultimately, protect their privacy. We have developed a virtualized on-demand infrastructure that stores data using provisioned services and lets users securely access that data from anywhere.

In our approach, users are issued a unique key by service providers

Published by the IEEE Computer Society

0018-9162/13/$31.00 © 2013 IEEE

during registration, much like the process for activating application products. When the client requests access to a user's data, the gateway verifies the user, determines the last cryptographic state of the information, and initializes the virtual infrastructure. Users control their information as well as who has access to their data. The encryption is seamless to users and changes algorithmically without user interaction; each session is encrypted differently.

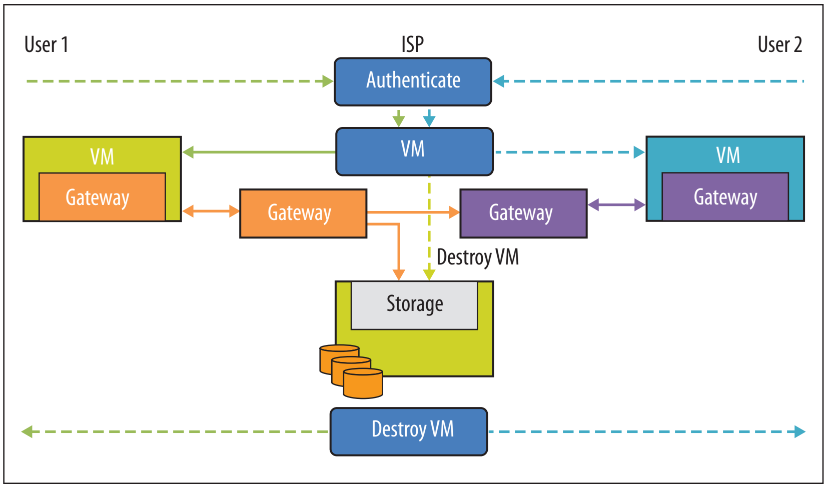


Figure 1. Data-centric security model. The two-level hierarchy of controllers denies malicious users the opportunity to locate data after a user session terminates.

DATA-CENTRIC SECURITY MODEL

Our approach's underlying data-centric security model consists of two types of trusted automated components: storage and communications.

The storage component encrypts (and reencrypts on a user-defined basis) user data, splits up the data, and then uses control gateways to determine where each piece of data will be stored in the service provider's storage area networks. To reassemble and decipher the data, the storage component manages metadata about the data's locations, the type of encryption applied to each piece of data, the type of data encrypted, and so forth. The metadata is encrypted as well, and users retain custody of the keys. The communications component connects the virtualized controllers to appropriate communications protocols for transmission.

A unique feature of our approach is that the storage and communications components are part of an on-demand infrastructure. Persistent global controllers, maintained by service providers, coordinate the actions of nonpersistent local controllers.

As Figure 1 shows, when a user creates data or accesses stored data, localized instances of the storage and communications infrastructure are activated in the form of virtualized controllers. When the user's session terminates, the corresponding local storage and communications controllers are destroyed. New virtual local controllers are dynamically created for each session. This two-level hierarchy of controllers denies malicious users the opportunity to locate data after a user session terminates because the local controllers' state information isn't saved.

Each user session consists of an encrypted network within the physical boundary of the service provider's network. The communications component manages the flows between the encrypted networks, whose plug-and-play nature prevents malicious users from exploiting common data flows—there are no "common" flows.

Our approach complements modern cloud architecture design, allowing the virtual infrastructure to expand and collapse as necessary. In the age of meshed networks, scalability is vital; no one owns all portions of a network. Therefore, to be completely secure, our method accounts for transportation of data across uncontrolled portions of the cloud.

Returning to Bellovin's second question, "Secure compared to which alternatives?," a virtualized on-demand infrastructure coupled with multidimensional encryption lets users retain control over their stored data and securely access it from anywhere. Our proposed approach can be realized on multiple cloud service platforms, is scalable across Internet service providers, and minimizes end user interactions, providing a robust security solution. C

Acknowledgments

The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements of the US government.

James Bret Michael *is a professor in the Naval Postgraduate School's Computer Science and Electrical and Computer Engineering departments. He is also vice president of engineering at Unified Data Solutions.*

Editor: Jeffrey Voas, National Institute of Standards and Technology; j.voas@ieee.org