Securing Dissemination of Sensitive Data and Documents

April 2015

Resilient Network Systems

100 Pine St, Suite 700
San Francisco, CA 94111
Telephone: (415) 291-9600

Securing Dissemination of Sensitive Data and Documents

The Challenges

Throughout government and enterprises, sensitive data sets and documents are routinely shared with other organizations, including suppliers, distributors, partners, and customers or citizens. While such burgeoning information sharing has led to much greater business efficiencies, once sensitive data is released to external parties, it becomes difficult to control the further dissemination of such data. This raises legitimate issues of protecting and potentially compromising intellectual property and personally identifiable information (PII), raising financial or legal liability, and even reputation issues for the organization that originally generated and then shared the information.

A number of existing solutions exist to address this set of challenges. Documents, for instance, can be electronically water marked, which while not precluding dissemination, enable a trail to be established regarding who held the document and to whom it was sent. More sophisticated digital rights management (DRM) solutions enable control of certain document types by providing static access control and limiting what users can do with a document. Even with such solutions, however, it is difficult to manage a data set or document that should be shared with multiple organizations in which the first receiving organization has a legitimate need to share the data with a third organization. Further, it is difficult for the original organization to change control policies for a document once it has been shared with external parties.

There is a need for a general-purpose policy capability that can protect all kinds of data sets and documents, and one that provides dynamic access control that is

determined by the original owner of the data. The policies protecting the data or document can be changed if necessary, and such changes will immediately be updated to protect all copies of that data set or document, no matter where such data resides at the time. Further, the policies should address the authentication of the individual to the level required by the owner, the authorization of the individual to see the data based on attributes or roles, and account for other context in the access control decision.

Solution Overview

To address these dissemination control challenges, a network-based policy engine can serve to provide access control and user rights to all types of data sets and document types. Without a network-based approach, such access control requires application specific changes that are static and often lack scalability for the enterprise and its partners. This network-based policy and access control approach relies on authoritative sources within the network for identity, access credentials, data, mission context, sharing policies and possibly behavioral analysis to evaluate policies that protect and appropriately grant access and usage rights to sensitive data sets or documents. This combination of authoritative sources combined with a distributed policy evaluation engine is Resilient Adaptive Access Management, capable of meeting these data and document dissemination challenges.

Solution Detail

Critical to the proper protection of a sensitive data set or document, a network-based policy engine, must first provide assurance of a receiving user's identity. The network-based approach offers several advantages. Since typically the receiving user will be part of a different organization than the data owner, a network- based identity validation model can readily check between organizations to reach authoritative identity stores (e.g., organizations' Active Directories) where the users are registered and thereby validate their status. This mitigates the need for repetitive federated identity management solutions or centralized identity stores. If multiple factors of identity verification are required, network policies can pose knowledge-based questions for authentication and connect to industry-leading providers of identity proofing. Or network policies can conduct an out-of-band phone or text authentication. If very high assurance levels are required, network policies can request a voice sample, facial scan, or fingerprint to

compare it to a known biometric. Within a mobile work environment, the policies could geo-locate the access device and cross-reference it to the GPS, beacon or WiFi readings from the device. If the login is from within an organization's facility, the network could check against physical access security systems to confirm the user is resident at the facility during the time of the access request.

Once the identity of the user has been established, it now becomes important to understand whether the user should have access to the data set or document based on their attributes and the context of the data or environment. The owners of a data set or document can establish policies for access based on the role or attributes of a user and the situation in which the information is being requested. Such policies will be invoked anytime a user attempts to access the data set or document, irrespective of their organizational affiliation. A network-based policy engine offers other benefits. For instance, as the environmental status changes (e.g., an emergency situation), data owners can change policies dynamically to allow or restrict data access or require additional validations, such as biometric access. Data security officers could also set policies based on threat levels issued by the Security Operations Center (SOC) such as requiring additional validations at higher threat levels. These dynamic changes can be achieved without requiring changes to the specific data sets or documents being protected.

Likewise, since a user's trustworthiness can change over time, policies in the network could be written to include input from systems that look for anomalies in a user's behavior. For example, the behavior analysis system could determine that a user's attempt to access certain data sets or documents is irregular. As an input to a policy in the network, this anomalous behavior could require phone authorization by a supervisor or the data owner prior to the user being given access to the information.

About Resilient Network Systems, Inc.

Resilient Network Systems makes adaptive access management software for identities you don't (or can't) manage. Our network-based, distributed architecture is highly flexible and scalable, allowing customers in government and enterprises to safeguard their data and applications, while enabling more collaboration and information sharing with their entire ecosystem. We make it simple to leverage existing identity and security products, or add external identity sources and services, with easy-to-implement, predefined and custom policies.

Resilient Network Systems is a privately held, venture-backed company based in San Francisco.