Combatting Insider Threats Using Behavioral Analysis and Network-based Access Control

January 2015

Resilient Network Systems
100 Pine St, Suite 700
San Francisco, CA 94111
Telephone:
(415) 291-9600
www.resilient-networks.com
Combatting Insider Threats Using Behavioral Analysis and Network-Based Access Control

The Challenge

Sensitive data is increasingly at risk. While hackers have become quite sophisticated, the compromising actions of trusted insiders have been the most devastating. In many cases, an insider is both properly authenticated through an organization's identity management system, and authorized access to sensitive data sources, that when exfiltrated, have potentially serious, negative implications for the organization. In other cases, an insider (or potentially outsider) compromises a legitimate user account and uses that account to move laterally within the organization’s systems to exfiltrate sensitive data. Most harmful are situations exemplified by Edward Snowden, in which a privileged user (e.g., system administrator) leverages their or other users’ credentials to exfiltrate data or in other ways work to harm the organization.

Solution Overview

To prevent the exfiltration of information and to ensure that only the right individuals can access data across a myriad of devices and environments, an innovative architecture and enabling technology are needed. By leveraging distributed network resources for processing access control decisions, a system can move beyond traditional methods for authentication and authorization, device-level security, or application-based access control to validate not only the user’s identity, but also other context appropriate to an access decision, such as data access credentials available from trusted sources outside an particular application. Further, this Trust Network, comprised of services and protocols in the network, can be combined with behavioral analysis tools or security information and event management (SIEM) systems to understand and use behavioral techniques as part of an access control decision. The innovative approach ensures that information is only made available to a user that has been behaving akin to normal behavior for a user in a particular role. Access is denied to a user if their network behavior falls outside a normal range. Such behavior could indicate either improper behavior on the part of that user, or that the user’s credentials have been potentially compromised. In either case, immediate denial of access is warranted while the organization conducts an investigation into the reason for the abnormal behavior.

Solution Detail

Insider threats usually involve the misuse of credentials belonging to privileged users or the escalation of privileges of a known user to achieve a privileged capability. Threats can come from a privileged user whose motivation has changed, or they can originate externally from someone impersonating a privileged user’s credentials. Validating the identities of privileged users, and understanding their behavior are essential to
Combatting Insider Threats Using Behavioral Analysis and Network-Based Access Control

combatting insider threats. Similar challenges occur when an organization is sharing sensitive information with other organizations. Information sharing across multiple organizations requires the ability to authenticate individuals outside of one’s own organization, adding to the complexity of properly authenticating and authorizing individuals for access.

Identity

As individuals connect to an organization’s network, the use of a Trust Network for identity validation offers several advantages. It can readily check between organizations to reach authoritative identity stores (e.g., organizations’ Active Directories) where the individuals are registered to validate their status. This mitigates the need for traditional federated identity management solutions. If multiple factors of identity verification are required, network policies can request a voice sample, facial scan, or fingerprint to compare it to a known biometric. Or network policies can pose knowledge-based questions for authentication and connect to industry-leading knowledge providers to provide identity proofing. To provide improved security, all data handled by the Trust Network can be obfuscated, and the adjudication of policies in the network is handled on a distributed basis, so there is no one point of compromise. Further, the policies for identity authentication are unknown to the user requesting access and the order of the requests can be randomized to further help prevent compromise.

Authorization

Once the identity of the user requesting data access has been established, it now becomes important to understand what data should be accessed. The Trust Network enables the data owner to define policies around authorization, classification levels, and mission context of the person seeking access. As emergencies occur, data owners can change policies dynamically to allow or restrict data sharing or require additional validations such as manager approval. Data owners can also set policies based on threat levels issued by the Security Operations Center (SOC) such as requiring additional validations at higher threat levels.

Behavior

Since a user’s trustworthiness can change over time, policies in the network can be written to include input from behavioral analysis systems or All-source Intelligence systems that look for anomalies in behavior. For example, a behavior analysis or SIEM system can notice that a privileged user is suddenly trying to move large amounts of data or files outside his or her normal context, or that several identities are logging in from the same computer. Before an individual is given access to information, a policy in
Combatting Insider Threats Using Behavioral Analysis and Network-Based Access Control

the Trust Network can require checking with the behavioral analysis system. If the behavior is unusual, a policy requiring phone authorization by a supervisor or the data owner can be invoked.

As a means to provide greater data protection while sharing information between organizations, links to the data can be shared with credentialed users in other agencies instead of replicating data between agencies. The information can be accessed when it is needed if the requestors meet the access credentials, context, and behavior patterns defined by the data owners. This design approach minimizes the transmission and replication of data across multiple data stores, saving on transmission, storage, administration, and synchronization costs between databases. Security is enhanced since the data obtained by the organization can remain at rest in the original data store.

About Resilient Network Systems, Inc.

Resilient Network Systems has built and launched the Trust Network platform to address the pressing need for secure and privacy-protecting access across the Internet. A Trust Network virtualizes real-world relationships and conditions of trust by confirming identities within the network, and enforcing each participant’s resource access policies while divulging the minimum required personal information. Both sides of any type of access, data sharing, or transaction event develop higher levels of trust due to improved authentication of each party and adherence to each other’s policy requirements. Resilient is based in San Francisco, California and maintains a second office in Washington, DC. The initial funding has allowed the core technology to be designed and built, initial revenues to be generated, and for three initial pilot implementations with large potential customers to be completed. The first production instance of the Trust Network supports more than 300 law enforcement organizations in Northern California. Learn more at www.resilient-networks.com