A Secure Cross-Agency Information Sharing Environment Utilizing Network-Based Credentialing Coupled with Voice Biometrics and XML Document Dissemination Control

November 11, 2014

Resilient Network Systems
100 Pine St, Suite 700
San Francisco, CA 94111
Telephone:
(415) 291-9600
www.resilient-networks.com
Evaluating Trust and Data Access in the Cloud

During the negotiations for the arms control treaty from 1985 to 1988, President Ronald Reagan often used an old Russian proverb in speaking to Soviet President Mikhail Gorbachev. Reagan quoted the phrase in Russian to Gorbachev to emphasize his meaning. Spoken in Russian, the phrase rhymes:

**Doveryai, No Proveryai, “Trust, But Verify.”**

With the rise of synthetic identities and identity theft, perhaps the policy should be reversed: “verify before trusting”. The need for identity validation suggests a new architecture where data access policies are network-based instead of application-based, and the identity validation is independent of the access device. This approach lets data owners establish and dynamically change access policies in the network, rapidly facilitating the formation and modification of communities-of-interest as circumstances change. Dynamic transactional trust evaluation enables attestation of the requestor’s credentials without the passing of personally identifiable information through the network. Risk reduction is accomplished by validating whether the individual requesting information should have access to sensitive data in order to accomplish a mission that is aligned with data owner.

Until recently, technology focused on validating a user to a mobile device and the device to the network. As mobile applications were developed, the data access policies tended to be imbedded within each of the applications. Such policies often necessitated multiple logins, which caused a lack of flexibility in the granularity of data that could be accessed by the users. The consolidation of information on the mobile device created a vulnerability that could provide a hacker with a target list for obtaining sensitive data if the device became compromised. Conflicting policies between applications and version control of applications provided additional challenges.

**Transformation:**

To transform productivity within an organization, data that normally resides deep within the organization needs to become accessible to front line workers so they can be empowered to make well-informed decisions. As organizational data is accessed from the network edge, it becomes critical to validate the credentials and the identity of the end user for each data request. Instead of point solutions, organizations should consider a “Trust Network” for network-based trust and identity attestation. Since the data access policies for each organization and partner are different and change dynamically based on situational events, it becomes critical to define data access policies in the network instead of in each application. For instance, law enforcement personnel access databases to obtain immigration status, identity information, and real-time assistance in identifying individuals suspected of criminal activity. By placing the access policies in the network, data owners could define the access credentials needed for each piece of data.
Evaluating Trust and Data Access in the Cloud

Each officer's credentials could be validated against network authorities including biometrics, such as voiceprint or facial structure, or behavior on a transactional basis. This would ensure that only authorized persons were accessing the requested data each time. Likewise, a Trust Network could enable the validation of credentials for pilots and employees prior to accessing flight data, schedules, and aircraft boarding on a transactional basis. It could also validate the identity of inspectors approving cargo screenings. The identity of First Responders and registered volunteers could be verified so that they could access resources in the event of an emergency.

Trust Network Technology:

Measuring trust requires a dynamic, transactional model for continuous evaluation and identity attestation that utilizes network-based policies in a decentralized architecture where the data remains at the source. It is a solution that transcends the mobile device type and operating system and can incorporate out-of-band authentication methods and the use of biometric data to validate identities.

Key Technology Considerations:

• **Peer to Peer** - A Trust Network needs a decentralized architecture with no central identity store, authorization service, policy enforcement point, or policy decision point
• **Scalability** - A decentralized design allows for massive scalability to incorporate growing transactional trust evaluation and identity attestation needs
• **Stationary Data** - By constructing a series of binary queries against authoritative sources, a Trust Network can eliminate the intercept and data corruption risks often associated with moving sensitive data through a network.
• **Authoritative Source Obfuscation** - The authoritative sources against which a Trust Network validates individuals needs to be unknown to the end device or user
• **Randomization** - By randomizing the order of validation against sources and varying the number of sources, a Trust Network deters pattern analysis and scripted attacks.
• **Protected Requestor Identities** - The requestor's identity needs to be protected using an attestation-based service that ensures access policies have been met without passing the requestor's identity.
Evaluating Trust and Data Access in the Cloud

- **Owner Defined Access** - Data owners need the ability to create network-based policies that govern the access of their data. This allows data owners to easily modify the policies in real time to reflect changes in circumstances.
- **Interoperability** - Network-based access policies need to work across mobile device types, operating systems, applications and organizations on the existing network infrastructure.
- **Common Language** - A Trust Network should provide a common language across multiple agencies and industries for policy creation.
- **Biometrics** - By incorporating voice prints and facial structure biometric matching on mobile devices a Trust Network can help determine the validity of the device operator “beyond the glass”.
- **Rapid Application Development** - Network based policies should enable rapid creation of new applications since the data access policies do not have to be coded into the application.

Implementing a Trust Network

A Trust Network requires identifying possible authoritative data sources for use in identity validation. The Trust Network should then connect with those authorities using a standards based interface such as Security Assertion Markup Language (SAML). Where possible, the Trust Network should leverage existing specifications such as the Global Federated Identity and Privilege Management (GFIPM) and the Backend Attribute Exchange (BAE) to normalize the required exchanges and address variations in identities and attributes. Properly deployed, a Trust Network should enable data stewards to utilize a web based, interactive GUI to create network-based polices governing the access to the data elements under their responsibility.

Access policies can include validations against network elements such as active directory queries, geo-location queries, out-of-band validations such as text messages to mobile devices with pin codes, personalized knowledge-based questions, and biometrics such as voice print comparisons and facial recognition to identify the individual. Additional contextual information from the network could also be included from security information and event management (SIEM) systems or log analysis systems to provide...
Evaluating Trust and Data Access in the Cloud

the necessary accounting in addition to authentication and authorization.

Evaluation by a Trust Network could also examine whether the data requester and their context has satisfied the credentials defined by the data owner, and if the permissions to access the data were granted or denied by the Trust Network. While Trust Networks may utilize proprietary software in their approach to trust evaluation and identity attestation, Trust Network providers should seek to actively build a “Trust Ecosystem” by integrating with cloud-based communities and by utilizing industry standards. Trust Networks should also seek to interconnect with authoritative sources and identity attestation services across both government agencies and private industry. Specifically, a Trust Network should offer EDI for supply chain integration and OFX for connectivity into the financial industry. In addition, Trust Networks should offer access through standards-based connectors, such as SAML, LDAP, and OAuth, or a REST-based API for custom integrations.

Empowering the End User

Having identified the data sources to be trust-enabled, the authorities to be utilized, and policies and credentials to be developed for accessing the data, organizations are ready to empower their business processes. For immediate availability, Trust Networks can be utilized as commercial-off-the-shelf (COTS) public, private, or hybrid-cloud solutions. Applications can be more rapidly developed since the policies governing identity validation and data access no longer need to be built into the applications themselves, but can be accessed through a proxy server as part of a defined widget within their agency’s or organization’s app store.

Sponsored By:

Resilient Networks
AcquSight
Nuance Communications
Industrial Medium Software

Point of Contact:

Brit Wanick
Executive Vice President
Resilient Networks
415-717-3899
brit@resilient-networks.com