InfoAssure, Inc.
The Trusted Source for Information-Centric Security

Persistent, Vigilant Data Protection
Anywhere-Anytime

INFORMATION-CENTRIC SECURITY (INFOCENSEC®)

How to Realize Object Level Self-Protecting Data Objects

For

Secure Virtual Communities of Interest (vCOI) Info-Sharing

2018

James G. Lightburn, CEO
InfoAssure, Inc.
j.lightburn@infoassure.net

InfoAssure, Inc.
www.infoassure.net

ABSTRACT

There is no doubt anymore that we are living in the midst of the digital information age and the Internet is a global village with everything and everyone connected. This is evidenced by our everyday use and dependence on instant on-demand information using the likes of the PC, laptops, netbooks, email, IoT networks, the Internet, Google, Twitter, Facebook, iPad and iPhone or Droid phones and the list goes on and on. So it should be no surprise to anyone by now that the most prized commodity is no longer the network or even the device but the data itself.

Your laptop gets stolen with a lifetime of family photos including precious baby pictures of your children, all of your personal information, including SSNs and tax returns, your private family medical history and so on. Which do you want back the most? Is it the laptop or the data? Of course it's the information. Obviously the need to secure our data and prevent information from reaching the wrong hands has become more important than ever before and takes on new light. We all want to control our own data now more than ever. Even our government understands this. Go look at the insider threats news on the OPM hack, the NSA contractor Edward Snowden or WikiLeaks.

Our society has become so dependent on the digital economy and on demand digital information that we need for our everyday lives, from military operations to health care or financial records, when it is gone or leaked unexpectedly, we have very serious problems.

Many have often said that information is power, but not unless you use it. To realize its full value, digital information must be discoverable, reliable, protected and shared securely. The evolving demands on information sharing drives the need for more sophisticated means of protecting and controlling access to information. This paper describes this evolution and the new requirements and set of challenges that it brings. An information-centric security solution is offered for consideration of creating and managing virtual communities of interest (vCOI) for info-sharing. The access control decisions are based upon a sliding scale of trust driven by policies, environment, user identification, roles/duty, and the metadata bound to the information object itself.

1 Introduction

Discretionary and/or mandatory access controls enforced within a local network have been the standard method of controlling access to data. But once data leaves the network and becomes mobile, this control is lost. So the traditional methods of protecting data are based upon preventing outside attacks or data from crossing organizational boundaries. In a word, it is ***net-centric***.

1.1 What's wrong with Perimeter and Net-Centric Security?

This perimeter based security or net-centric approach fails when data must be shared across the network boundaries and without sharing; the value of this data is minimized. Some say that secure cross-domain communications are possible but then assume that the other side of the boundary is a trusted environment with trusted users who will protect the data. Experience has shown that, although in concept this is a good solution, in practice it falls short. Especially when new cloud based sync and file sharing is used such as Box or Drop Box. Control of information is inherently lost when crossing boundaries and setting up trusted environments between any two, let alone many groups can get bogged down in politics as the case is with multinational military operations in Afghanistan, Iraq and the ongoing fight on terrorism.

However, all organizations partner with others to a greater or lesser extent to get work done; the term "hub of commerce" is sometimes used to describe this partnering in commercial. Information must flow to other entities outside of the owning organization. It is very hard, in general, to control where information goes once it has left the local network. So rather than control the physical flow of information, it is more efficient to control the access, i.e. who gets to see and use that information when and where.

1.2 Hubs of Commerce, Coalitions & Communities of Interest (COI)

In recent years, wars have been fought with many nations coming together on one side. Coalitions have been formed. The need to share sensitive information among the coalition always arises. However, the physical means of sharing information is overtaking the logical means to limit access in a timely manner. It is not so different than the many organizations in a commercial customer driven hub of commerce.

When information needs to be shared among a group of individuals from different organizations to achieve a common goal, a "Community of Interest" (COI) exists. Participants in a COI have a common interest of sharing information, yet still insuring its security. It is a dynamic group; individuals, organizations and other participating entities come and go periodically, even daily. Given the dynamic nature of these groups, access controls must not only be applied across the whole COI but also be enforced based upon changing policies. The ability to modify access and even take it away must remain with the owners of the data (the originators, managers, or their delegates). Furthermore, a means of discovery, i.e. being able to pick out what information is needed from the plethora of data that exists, must be provided to the COI. The data and its discovery must be timely and accurate.

An example of a COI is the need to share national intelligence information with state, local and tribal authorities in threatening situations. The local authorities only need to get information pertinent to their role or duty also known as area of operations. They should not, in fact, see data that they do not have any need to know.

On the other hand, local law enforcement and emergency authorities should be able to provide input up to the national intelligence system itself.

It is appropriate for national authorities to control access, and to gather and coordinate input from the local areas. So, while all parties can share information, one of these entities may still maintain organizational control.

1.3 Digital Rights Management and Malware

Once information leaves the local network there is no way to recall or delete it. "*You cannot recall email once you've hit the send button*" is a phrase which we are all familiar with. And so is the maxim that hitting the "delete" button does not really delete data. As much as we would like it to succeed, digital rights management (DRM) has not been able to control access to data once it has left the hands of their owners.

The status quo security model also leaves a lot to be desired in terms of ensuring the accuracy and reliability of information. When current security paradigms were created data was controlled within one machine and operating system. Later, computers started to be connected together into local networks. Then it happened: these networks were connected together and the Internet was born. As the Internet and its use has matured, so has the evolution of malware and denial of service. Many business processes need to make decisions based on accurate, time sensitive data. Information dominance cannot be achieved in this hostile Internet environment without data protection, which unfortunately cannot come about in a net-centric security model.

1.4 Trusted Insider Threat

Then there is the "trusted insider" threat where a trusted individual turns out not to be trusted, as has been so amply demonstrated in news articles [1] time and time again like the Edward Snowden the NSA contractor who stole classified information and leaked it to the world. We have found that ***people steal data not computers***. The only reason that these people have been "trusted" is because the access control mechanisms are based on an all-or-nothing concept. If someone is cleared for access then they get to see all the information on the network at the level for which they are cleared and below. Personal identity information (PII), medical records, credit card numbers, and so on must likewise be protected as mandated by law. But access to this information has been ill-managed resulting in security lapses, incidents and crimes. Ideally, access should only be given to data for which a user has a need to know.

Fine grained access controls are what is called for, i.e. the determination of granting or denying access is based, at least in part, on identity. Access Control Lists (ACL) placed on data is one such solution. But this places a burden on managing these resources.

1.5 Existing Approaches

Role-based access control (RBAC) has been put forth as one method to make fine grained access control manageable. Other techniques have recently been proposed, such as attribute based access control (ABAC) where access decisions are based on certain "attributes". A further refinement of this concept is policy based access control (PBAC) where access is governed by policies that are more sophisticated than just examining a small set of attributes. A policy enforcement point (PEP) queries a policy decision point (PDP) which decides whether access is granted or not. The PEP then acts on the decision. Risk Adaptive Access Control (RaDAC), adds real-time risk assessment to the decision logic.

What these methods – ACL, RBAC, ABAC, PBAC, and RaDAC – have in common is that they are designed to work within the boundaries of a controlling organization. However, lessons learned from various recent commercial and government pilot programs have identified numerous shortcomings even within the organization. As organizational complexity increases, so do the management of roles, attributes and policies [9]. There is no standard used for applying metadata to aid discovery, analysis and processing of the data. Subject attributes tend to be specific to an enterprise rather than something that can be captured in a general access control system. And policies are hard to identify and use.

1.6 Requirements

To summarize, data access must be controlled in an efficient, fine-grained, timely, yet easily manageable form, and must maintain enforcement once the data has left its local domain of logical control. Clearly some form of metadata which describes the accesses allowed and by who, and furthermore is bound to the data object[1] itself is necessary. Automated control should be applied to limit access based upon this metadata while the object resides in storage, during transit and after it

[1] The term "data object", or just "object", in this paper refers to any set of (usually binary) data. This can mean computer files. However, it may also mean communication streams, documents, directories, paragraphs, lines or words in a document, even folders and software programs.

leaves the boundaries of the originator's organization. Control then cannot be net-centric. **It must *be information-centric***.

How can this be done without burdening the data object with large amounts of metadata – especially when the list of potential users who are given access is large, roles are dynamic, and policies are complicated? A solution based upon cryptography can be the basis for enforcing access control. The problem is then transformed into managing cryptographic keys.

Fortunately, the clever use and management of encryption keys can simultaneously provide confidentiality and granular access control of both users and data objects.

2 A Solution Attempt

In a recent paper by Burnap and Hilton [2], a solution using cryptography is proposed. In the approach described each document is encrypted. The cryptographic keys are stored in a central database. A Java tool is used to query the database with the user's credentials, decrypt the document and present those portions of the document that the database has determined the user has access rights.

The intent is to realize a concept introduced in the paper that they term ***de-perimeterization.*** This refers to the need to control access at the point of access, as opposed to having it determined as it leaves the boundaries, i.e. at the perimeter, of an organization. Perimeterization can be said to be the traditional net-centric approach; de-perimeterization the information-centric approach.

The need for de-perimiterization is brought about by the formation of "*Virtual Organizations*"(VO), the term they use which is roughly synonymous with hubs of commerce, COIs and coalitions. The proposed cryptographic solution tags the encrypted information with persistent metadata representing access control requirements. Access is controlled by mapping users to these tags in a centrally located database.

The system described in the paper is in its early stages and the authors point out areas that need more study and development. Nevertheless, there are certain implementation aspects that lead to unfortunate characteristics that cannot be solved without changes to the underlying design decisions.

The policy in the system described is not flexible, identifying Boolean values (yes/no) for only four controls in its initial development, viz. community access, restricted access, personal information and organization only. It is conceivable that more controls will be added in the future, however, these controls are basically static in that they are defined at the development layer as opposed being defined and managed at the implementation layer. Furthermore, access is either granted in full or not, i.e. an all-or-nothing answer. Although a user can add to the content and classification labels, and parts of the protected data can have different classifications, there is no way to limit access to write-only or read-only. Maintaining the keys for every protected document in a central location also affects scalability and provides a single point of failure.

3 Using Cryptography

If the cryptographic solution proposed above cannot fully meet the needs of information-centric security, then what is required of a cryptographic solution?

3.1 Persistent Access Control

Some formats already exist for adding access control information to data objects. XACML is one such standard based on XML, a well-known, flexible method of adding metadata. Access control with XACML is enforced by algorithms that make access control decisions based upon policy contained in the metadata. Although not ruled out, encryption is not usually part of the access control enforcement and a trusted computing environment is needed to ensure adequate enforcement. This environment includes a PEP that usually must be at the operating system level. The PEP does not determine access itself. Rather it gathers information about the user and (maybe) the environment and sends requests for an access decision to a PDP, which may be at another location. XACML is used to realize ABAC and PBAC type of controls. However, network infrastructure must be added for XACML to work and this can affect scalability and management as well as cost.

Another standard way to add metadata is to use the Cryptographic Message Syntax (CMS[2]) which is specified with ASN.1[3] and encoded in a binary format. It's not human readable but uses cryptography as implied by the name. It is more compact than XML, and is flexible enough to freely add users to the "read" list as long as these users each possess a cryptographic key pair. Infrastructure is needed for management of these key pairs and is usually implemented with a Public Key Infrastructure (PKI). When used in a virtual organization, many potential users may need access and this brings up two problems – scalability, and the requirement that the author have

[2] The IETF standard RFC 5652[3] is the current CMS standard (it is updated periodically). Other such standards are PKCS#7 (which is the original CMS), ANSI's X9.73 and S/MIME, as are others based upon CMS.

[3] Abstract Syntax Notation One

access to the public keys (certificates) of users that the author may not know.

3.2 Scalability

Adding users to an access list one by one is bound to get unwieldy and in fact, untenable when trying to collaborate beyond organizational boundaries. The way out of this is to use groups, i.e. broad categories of access. This will cut down the amount of metadata to be carried around on a protected object. And rather than knowledge of individuals, the knowledge of the group and its purpose is what is used to establish access policies on an object.

One obvious access category to use as a group is sensitivity. The Bell-LaPadula model [4], which formally describes security policies of military and intelligence systems, basically states that in a multilevel security environment a process may only allow information to be read at the clearance level of the user or below (*no-read-up*). It also states that information at a certain level can be written by those with a clearance at that level or higher (*no-write-down*). This provides a policy for managing access at different sensitivity levels. One way in which cryptography can be applied is to use cryptographic one-way functions to derive keys going down in sequence from high to low sensitivity. A user needs only one key value at their assigned clearance level. Keys used to protect lower levels will be derivable from the user's single sensitivity level key. Higher levels cannot be derived based upon the mathematical one-way-ness of the derivation function. Note that no trusted environment is needed, only cryptographic applications, in this case to enforce the "no-read-up" policy. A secure cryptographic module should be used for confidentiality, but access control enforcement is inherent with this approach.

Another obvious category would be, say, "project". Those working on a particular project would be given access to objects encrypted with a cryptographic key shared by those on the project. In fact, users may have access to several group keys. For example, a particular user will have the keys to, say, the secret group and the project X group. Another may have keys for the top secret and project X groups. These keys can be named for convenience. When used for encryption of an object we will call these keys labels.

Label keys must be able to be created when needed. This is a management function, and being part of a key management scheme, needs to provide all the capabilities that key management entails. To achieve a high degree of granularity, different defined/named categories of labels can be used to group and partition labels to make management, use and revocation easier.

3.3 Access Granularity

Group keys are a useful concept and their use to implement an RBAC system is intuitive – use shared cryptographic keys for different roles. A user playing a particular role will possess that shared key. RBAC has been used with success, however, sometimes more sophisticated logic needs to be used to implement the desired access policy, especially within a virtual organization. How can the access control on an object be broadened or restricted to tailor access?

In formal logic the concept of a Disjunctive Normal Form (DNF) arises. Statements are connected using the prepositions AND, OR, and NOT. DNF is a canonical form that is easily understood by those tailoring access controls and easily processed by a computer. A DNF formula consists of one or more "conjunctions", i.e. statements connected with the AND preposition. Each conjunction in the DNF statement is then interpreted as being connected with the OR preposition[4].

As an example, we want all those with a secret clearance AND those who are actively working on project X to have access to a particular document. This results in a single conjunction, viz. (secret AND project X). But we could also say we want those with a secret clearance working on project X OR project Y to have access. In this case we need two conjunctions: (secret AND project X) OR (secret AND project Y). Note the two conjunctions and the fact that they are connected with an OR.

Adding labels within a conjunction, i.e. ANDing them together, for access on an object will result in decreasing readership of the object. On the other hand, adding conjunctions to the DNF set that are OR'ed together increases readership. This is a way to finely tailor access control policies.

Another, possibly more intuitive, form is the inverse of DNF, called Conjunctive Normal Form (CNF). In this case it is disjunctions that are ANDed together, each disjunction being a set of label(s) that are OR'ed. The above example would then look like (secret) AND (project X OR project Y). Both form is valid and it is an easy matter to convert from one to the other in software. Whether one is more desirable than the other becomes an implementation issue. Henceforth, this paper will only talk in terms of DNF.

In summary, using formal logic, it is possible to simultaneously apply several labels in order to tailor the audience, either increase or decrease readership, for protected objects and truly achieve fine-grained access control and create circles-of-trust.

[4] **Note that the not modifier is not used in this case. Nevertheless, this is still DNF form.**

3.4 Dynamic Management

Now we are able to add fine-grained access controls to objects that persist with the object and are able to leave the boundaries of the originating organization without losing this control. However, as pointed out in the Burnap paper, a way to dynamically change access policy is still needed. Can applying cryptography to protected objects still provide this dynamic control?

Remember that once the data object has left an organization there is no way to control the document per se. But controlling the keys that a user has is possible. In short, by giving a user access to a group key, that user is being granted access to data encrypted with that key.

The need to control a user's access to cryptographic keys has arisen. One way to do this, of course, is central management of the user-key correspondence as in the Burnap paper. This has the downside of dependence upon the database by users causing scalability problems and having a single point of failure. But actually, the management of keys and users are separate. Access to the label keys can be realized by placing the keys on other servers that can be reached by users. By doing so redundancy and federation can be applied resulting in better availability and scalability.

Another great advantage of federating label keys on servers is that by deleting these keys, a user's access to protected data can be revoked with the click of a computer mouse. Also, intelligent placement of these labels can restrict users to certain locations and even networks. But now the question arises as how to protect these cryptographic keys.

3.5 Cryptography

Here again, cryptography can provide a solution. Label keys can be encrypted using asymmetric key cryptographic functions, i.e. public key cryptography. Labels are placed on repositories (basically file servers) encrypted with a public key that is associated with each user. The user possesses the private part of the key and is the only one that can decrypt the labels encrypted with the public part.

These encrypted label keys can to be replicated across the label key repositories. However, if label keys are replicated then the key on all of the repositories for a user must be erased to revoke a user's access to that label. This can be taken another step further.

Another type of cryptographic primitive is known as secret sharing. It is normally implemented using a threshold scheme. A (t, n) threshold scheme[5] specifies that a value be split into n different values such that no less than t of these values must be known for the secret sharing function to be able to recreate the original value. For example, using a (2, 5) threshold scheme to split a user's label key value means that five values will be created, such that any two of these are needed to recreate the original label key value. If these "splits" are placed on five different servers then erasing four of these values will be sufficient to revoke a user's access to this label key. The (t,n) values can be varied to control redundancy and ease of revocation. This is particularly important when the controlling agent cannot reach all of the servers for one reason or another. Enhancing the threshold scheme with another parameter to form a triple, (m, n, o), can be used to make this capability even more convenient. The (m, n, o) means that a (o, n) threshold scheme is being used but that m (mandatory) specific splits are needed in addition to the o (optional) splits to recreate the original value. For example, a (2, 1, 5) scheme means there are five splits created, the first two of which must always be present to recalculate the original value (the mandatory splits), plus one of the remaining three (optional) splits. Placing the mandatory splits on a machine guaranteed to be accessible to the controlling agent will ensure revocation ability. The optional splits are then placed on servers that can be used for redundancy and availability or for restricting the user to certain networks, for example.

4 Cryptographic Key Management

This paper has been advocating the use of cryptography to manage access to data objects. Cryptographic key management then becomes paramount if the system is to be secure. Key management issues need to be solved. This document will not discuss all of these issues; however, some of these are touched on below.

Public-key cryptography is leveraged to ease management. But unlike PKI, personal keys need not be managed with certificate revocation lists (CRL) or with the online certificate status protocol (OCSP). This system only depends on centralized management functions, thus allowing revocation and access re-assignment to be done in one place. However, this central management is not needed for day-to-day access control – it is only needed for changing the user access permissions. Users will communicate with other, likely multiple, redundant servers (user label repositories) to access their label keys.

In practice, data is encrypted with a random secret key and label public keys are used to wrap (encrypt) the data encryption key. The Cryptographic Message Syntax (CMS) standard possesses the capability of supporting this mechanism as well as the DNF required to realize fine-grained access control. This same scheme

[5] *See, e.g. Stinson[5], pg 337 - 333*.

also has the potential to provide XACML the same capabilities but research is ongoing at this point. Details will not be provided in this paper.

Another issue is the binding of label metadata to an object. Simply including the metadata in a digital signature with the protected data will suffice. Personal digital certificates are then used only for the digital signatures, not for encryption.
Resulting security is then less sensitive to a CRL. Whether a certificate has been revoked has no bearing on encryption and access control since the key used as outlined here need not be bound in a certificate. Only the fact that a certificate was valid at the time that the data was signed is necessary.

Finally, the ability to vary key values regularly or if they become compromised is a necessary requirement. Data encryption keys as referenced above, always have differing values by virtue of the fact that they are created randomly. But by judicious use of cryptographic one-way functions label key values can be varied with a minimum of storage requirements, generally one or two values to generate a whole sequence of label key values. Furthermore, this scheme can be extended to bracket user's access to specific editions of label keys, for example to a certain interval of time, providing further flexibility.

Other aspects of key management are necessary but are not in the scope if this paper and will be addressed in future documents. The point here is that key management and fine grained access control go hand-in-hand.

5 Summary

We have outlined requirements for sharing digital information across domain boundaries that preserve access controls based on policy and roles defined by the owner of the data. Ways to implement a solution to these requirements have been discussed. Here is a summary of what has been presented.

5.1 Crypto Labels

Encrypt data using labeled keys that have been provided by centralized management. Labels are intended to be used for groups of users. When one is applied to encrypt a data object then those who have been given access to the label key has access to the data object. The owner of the data need not know who specifically is in the group, only that those who have access to the label have access to the data.

Multiple labels can be used to tailor access and can realize fine-grained or more general access controls as needed by the owner of the data. Access can be controlled for reading, i.e. decryption (the private part of the label key) and writing, i.e. encryption (the public part of the label key). Furthermore, a hierarchy can be arranged so as to separate data at different sensitivities in a multiple level access control system.

5.2 User Management

Robust user identification and authentication (I&A) is naturally needed for such a system to be secure. In a multi-level access system, different I&A policies should be applied to different levels. I&A requirements and solutions are outside the scope of this document, but using labels for sensitivity can offer a multi-level solution.

Management of users is controlled at a central location. Since access depends on access to label keys by users, management is concerned with individuals' access to these keys, not with their access to the data. Access to actual data objects is controlled by the author or owner of the data, or by organization-wide policies. Individuals' access to label keys, and hence access to the data encrypted with those labels, can be changed immediately. In fact, taking away access to all label keys results in effective revocation. Label keys for individuals can be placed in multiple places resulting in redundant availability and/or tighter control.

5.3 Audited Access

What has been described above then is an efficient, fine-grained, timely, easily manageable, globally enforceable method of controlling access to data that can be shared within any type of virtual organization without losing that control.

Access can be controlled by policy based on attributes that include labels. Labels themselves can represent various types of attributes. Therefore, this system can realize ABAC and PBAC types of access control mechanisms. Label meta-data on objects can allow secure discovery of data as well as allow for efficient auditing.

5.4 Managed Membership

Labels are grouped and these groups are assigned to users for different roles at different times and places. These attributes can be incorporated into different levels of I&A policies, thus realizing the dynamic changing of roles and implementing the idea of different cyber presences for an individual as well as aiding multi-level security. I&A policy can be applied to require the use of digital certificates and the system should not only co-exist with a PKI but should also use any existing PKI leveraging existing X.509 certificates and X.500 directories (such as LDAP and active directory) to automatically assign labels and roles to users. This allows COI's to be set up in a very dynamic way, importing groups of users as well as revoking membership in a COI for a whole group of users. This management can be centralized within one organization or distributed throughout several organizations.

5.5 Self-Protecting Data

In the self-protecting data model, the need for any net-centric security protection is minimized. Data is persistently protected whether it is in-transit through a network or at-rest on a computer disk, a thumb drive or on a CD/DVD. Only successful I&A at the appropriate sensitivity level will allow users to have access to the appropriate keys that will allow decryption of the data.

The information-centric solution embraces the definition of self-protecting data and when implemented can result in a very large cost and performance savings across the info-sharing enterprise.

6 Need2Know®

InfoAssure, Inc.[6] has been researching and developing such a privacy platform for several years. The tool is called "Need2Know®", or simply N2K. Implementations and pilot demonstrations have taken place and have been successful. In Coalition Warrior Interoperability Demonstration (CWID), 2008 and 2009, the N2K technology was the core capability inside of the USSOCOM (US Special Operations Command) demonstration called Classification Stateless Trusted Environment (CSTE). In CWID 2009 the CSTE-N2K demo was picked by DISA as a top 5 technology selection. This is an implementation of the patented [6][7][8] cryptographic key management and access control system as described above.

There is an administrative portion which is used to manage labels and users access to them. There are client programs for encrypting and applying access controls to computer files and directories, encrypting voice and video streams, adding access control to instant messaging and SharePoint repositories. A software development kit (SDK) is offered to allow developers to enable their applications to use N2K. The system is implemented using standard computer languages, e.g. C, and can be implemented in dedicated hardware. It is implemented in modular form and is intended to meet FIPS 140 security module requirements. Finally, there is an enrollment system to register users into an N2K organization.

A further component is supplied as part of the SDK: a user Identification and Authorization (I&A) component. The administrative component allows different policies to be set for I&A at different sensitivity levels and accommodates passwords and passphrases, physical tokens and biometrics. The client portion enforces these policies. As in the rest of most of the system, cryptography is used to enforce I&A.

The cornerstone of N2K capabilities include the setting up of coalitions or communities of interest that allows two or more organizations to securely share data. This is exactly the concept of the VO described in the Burnap paper. Each organization must have an N2K implementation and agree to collaborate. One organization, called the host, has the capability of managing the coalition and hence is the controlling agent, creating and allowing the other organizations in the coalition access to the coalition labels. Each guest then assigns its users access to these labels as they see fit. In a COI, management can be transferred to different organizations or other controlling agent very easily and quickly to support the dynamic nature of the COI.

For simpler, one-off data sharing, one N2K organization can export the public key of a label to another giving the second organization encryption capability for data that members in the first organization can decrypt. Exporting a label public key from the second organization to the first will allow two-way secure communications.

N2K goes further than the system described in the Burnap document. De-perimeterization and granularity of access control are still maintained with this information-centric solution. Data is encrypted and the vulnerabilities of releasing data outside of the traditional boundaries of control, whether accidental or malicious, are mitigated to a good degree with trusted self-protected data objects.

Following the principles of cryptographic defense-in-depth key management and allowing I&A to be tailored by crypto label management and enforced at different sensitivity levels by binding the labels directly to the data object results in a robust and granular access control system that meets the future secure vCOI information sharing and privacy compliance needs of virtual organizations today.

The N2K crypto labeling process transforms any data object regardless of its source application into a self-protected trusted object and empowers the data owner to control who can see what data on which device when and where.

[6] *See* www.infoassure.net

About the company:

INFOASSURE.COM, INC., is a privately owned emerging software technology company located in Chestertown, Maryland. The company's original focus was on Cyber Warfare and Information Operations (IO) providing classified IO services for US Government customers. Post the tragic events of the 9-11 attacks on our Homeland, the company transitioned into an Information Assurance (IA) R&D operation and conducted primary research and development focused on software technology for **Information-Centric Security (InfoCenSec®) solutions to enable trusted information sharing** solutions and creating virtual communities-of-interest (vCOI) with Circles-of-Trust™.

The company has three core patents covering cryptographic key management and information-centric security cryptographic labeling. The company's flagship software privacy platform is called ***Need2Know® (N2K). N2K*** embraces the **InfoCenSec®** model. N2K software is a crypto labeling process and cryptographic key management that provides both persistent privacy always on enforcement and access control of data at the object level in a single user application. N2K crypto labeling process is application independent and can be used to label and protect mobile data stored in the cloud or any other digital asset.

The N2K crypto management system leverages open source asymmetric and symmetric encryption libraries which are NIST FIPS 140-2 certified. Both forms of encryption are implemented in the N2K client application to provide multi-layer encryption of the object resulting in both access control and privacy protection. This process enables the need-to-share on-demand information at an enterprise level in a single or multi user device environment. The N2K software has a software development kit (SDK) with the API libraries. The SDK and APIs are available under an OEM technology license agreement for the integration of N2K functionality into OEM products and system integration engineering solutions.

For more information please contact:

James G. Lightburn, CEO
InfoAssure, Inc.
Tel: 410-757-4188-o 410-991-9611-c
Email: j.lightburn@infoassure.net
URL: www.infoassure.net

References

[1] Poulsen, K., Zetter, K., "U.S. Intelligence Analyst Arrested in Wikileaks Video Probe". Wired. At wired.com.

[2] Burnap, P., Hilton, J., "Self Protecting Data for De-perimiterised Information Sharing". IEEE Computer Society, 2009.

[3] Housley, R., "Crytographic Message Syntax". IETF RFC 5652, 2009.

[4] Bell, D. E., LaPadula, L. J., "Secure Computing Systems: Mathematical Foundations and Model," M74-244, The MITRE Corp., Bedford, Mass. May 1973.

[5] Stinson, D. R. *Cryptography: Theory and Practice*, CRC Press, 1995.

[6] G. D. Kimmel, F. J. Adamouski, E. L. Domangue, W. R. Kimmel, J. G. Lightburn, L. R. Viola, "Cryptographic Key Management", U.S. Patent # 7,711,120 May 4, 2010.

[7] G. D. Kimmel, E. L. Domangue, F. J. Adamouski, "Information-Centric Security", U.S. Patent # 7,715,565 May 11, 2010.

[8] G. D. Kimmel, E. L. Domangue, "Cryptographic Key Construct", U.S. Patent # 7,739,501 June 15, 2010.

[9] Sinclair, S., Smith, S., Trudeau, S., Johnson, M. Portera, A., "Information Risk in the Professional Services – Field Study Results from Financial Institutions and a Roadmap for Research".