Seeing the Real World: Sharing Protected Data In Real Time

John R. James
United States Military Academy
John.James@usma.edu

Frank Mabry
United States Military Academy
Frank.Mabry@usma.edu

Kevin Huggins
United States Military Academy
Kevin.Huggins@usma.edu

Abstract

We describe a new capability for "owners" of protected data to quickly and securely share real-time data among networked decision-support and real-time control devices with whom the "owners" of the data have explicitly decided to "share the data. The service is based upon implementation of a recent formal definition and mathematical result (James et al. 2009) derived from the decades-old Bell-LaPadula information security result (Bell and LaPadula, 1973). The service provides decision makers a means of securely and automatically sharing critical information across security barriers based upon declaration of sharing policies. The declaration and implementation of information sharing policies based upon a need-to-share has been shown to be compatible with information protection policies based upon a need-to- know. Indeed, the implementation of the need-to- share service is based upon extending the mathematical foundations of need-to-know information security systems (the Bell-LaPadula result of 1973).

1. Introduction

The flowing valued information (FVI) project is a three-year project supported by the Army Research Office (ARO) to investigate scientific barriers to sharing information among coalition partners involved in counter-insurgency (COIN) operations and nation- building efforts[1]. The FVI project has developed a support service termed Need To Share (NTS) (James et al., 2009). This service allows groups to share information with each other (at the group level) in a secure manner via a repository service. An IATT (interim authority to test) request for operation of this software on the Defense Research and Engineering Network (DREN) network at USMA has been approved for a test in the Summer of 2011 to share data among the National Military Academy of Afghanistan (NMAA) in Kabul, Afghanistan, the United States Military Academy (USMA) at West Point, New York, and the Royal Military Academy Sandhurst in Surrey, England. A student capstone engineering project at West Point (Lanahan, 2011) has built a user-friendly interface to enable "owners" of information to share desired data and to designate whom the data is to be shared with. Additionally, extensions to the basic capability are being built (Huggins et al., 2011) to implement the service on smart phones and other mobile devices. This paper summarizes the formal result which forms the basis for the information sharing service and provides details concerning real- time extensions of the existing service. The next section provides an overview of the formal result and the following section describes the existing service. We then describe the real-time extensions and conclude the paper with a summary section.

2. Formal Extension of the Bell-LaPadula result

The original Bell-LaPadula result was based upon general systems theory available at that time. The primary distinction to be discussed in this paper is the extensions necessary to formally consider real-time systems. That is, while Bell and LaPadula considered a system in its most general form to be a relation on abstract sets, the modern system theorists add consideration of continuously-varying systems as well as compositions of discrete, set-based, systems and continuous systems. Functional concepts of a mapping from one state space (the domain) to another (the range) remain the same. While Bell and LaPadula considered the system S to be a relation on the abstract sets X and Y, Lee and Varaiya (and others) consider the general system S to have elements which are members of abstract sets and also elements which are members of general functional spaces (Lee & Varaiya, 2002). The mathematical details of the extensions to the Bell-LaPadula model are too

978-0-7695-4525-7 2012

DOI 10.1109/HICSS.2012.518

lengthy to be provided here. However, the mathematical details are

available on-line. The on-line report provides mathematical details on (1) extending the models of the systems being analyzed to include what are described today as "complex systems" and (2) extending the existing Bell-LaPadula model for defining a failure to secure information (a security compromise) to include defining a failure to share information (a sharing compromise).

The mathematical result follows current system theory (Lee and Varaiya, 2002) results in modeling and analyzing systems which are compositions of logical and continuous system components. Associated with the current systems theory models are rigorous definitions of continuous and discrete states and associated models of continuous behaviors and discrete behaviors and hybrid (combination of continuous and discrete) behaviors. These behaviors consist of continuous, discrete and hybrid trajectories from a set of initial states to a set of final states. The complete power of the hybrid modeling approach is not needed for each component (and may not be desirable!). For some (maybe most) of the components, a discrete model such as that used by Bell and La Padula is sufficient. Likewise, for some components, a continuous-system model is sufficient. The hybrid model is used when the future states of the composed system includes parameters of interest which exhibit both discrete and continuous behaviors (evolutions). We are convinced that for our particular problem space (decision support systems and real-time control systems), the hybrid model is generally required for capturing the range of parameter values of interest for complex system evolution. Our problem space of interest in this paper is that which can adequately represent tactical-level military operations where success in humanitarian assistance/disaster recovery (HADR) operations requires reasoning about trustworthiness of information elements to be flowed between distributed information nodes in a manner which (1) increases the value of information available for goal-oriented decisions in accordance with the intent of the commander taking into account that some of the information elements vary continuously with time and space, and (2) which complies with a command decision to share information. It is interesting to note that addressing item one above (flowing valued information) was a subject of discussion at the time the creators of the original Bell-La Padula model were working on their model (Bell D. E., 2005), (Landwehr, Heitmeyer, & Mclean, 1984), (Denning, 1976), at least in terms of seeking to analyze information security in terms of information flow. While this paper seeks to extend the framework of Bell and La Padula in terms of a formal treatment of general systems modeling and information sharing, we remark that the implementation details, in addition to following the Bell-LaPadula extensions in terms of

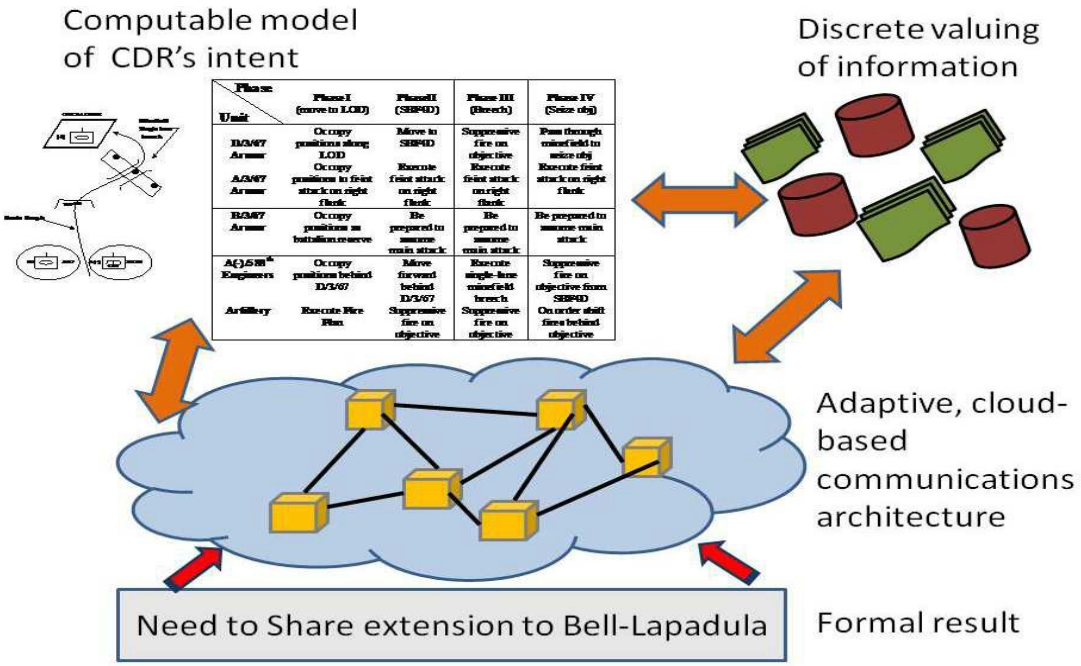

Figure 1. The need to share project

information security and sharing, will also be achieved as extensions to the current military messaging systems in terms of information flow between network nodes. As indicated by John McLean, there has long been considerable interest in fashioning the treatment of security in the same manner as Shannon had done for information theory by establishing the science for determining channel capacity (McLean, 1990). McLean's treatment of information flow considers bi- directional flow of information as preserving security for causal systems if the security state of the information object of interest is considered at different instances of time. However, McLean's treatment does not consider continuous values in time and space and also does not consider the case in which information value decays over time or distance from where it is most useful. Bell's review in 2005 of the Bell- LaPadula model states: "Consideration of access modes led to the unexpected identification of a hard-to- name information flow property, the star property. The relation W that conceptualized allowable changes of state was not constructive and was therefore insufficient for the analysis and formulation of core system calls that change the security state. (Bell D. E., 2005)" The star-property refers to the basic constraint of information flow across a security level in the Bell- LaPadula model as allowing "no read-up, no-write- down" operations (Figure 1 and Figure 2 of Bell D.E., 2005). Thus, decision support tools available to commanders today continue to rely on security models which restrict analysis to parameters whose values are members of sets. This restriction does not enable

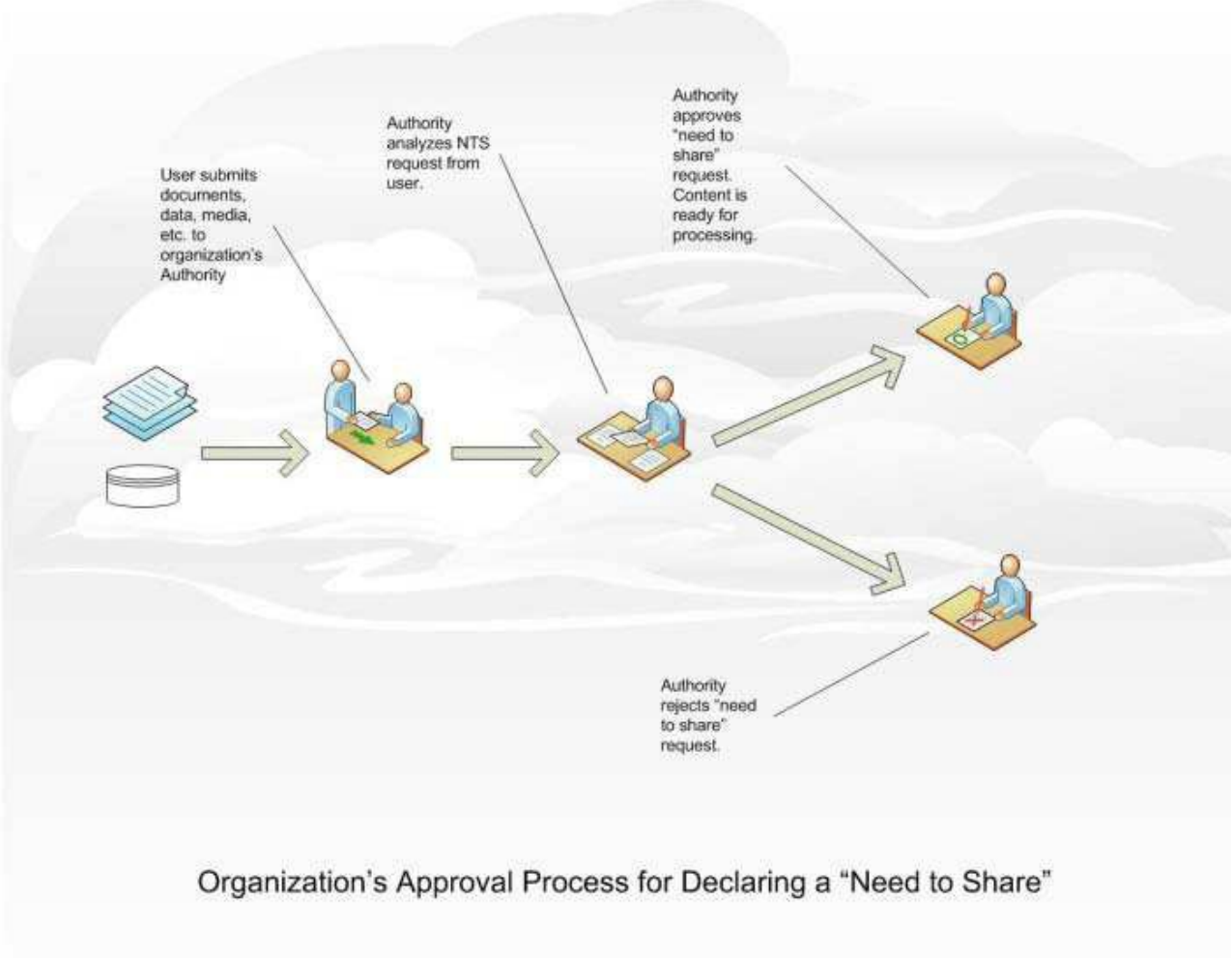

Figure 2. Selecting information to share is an organizational process

reasoning about parameters of interest whose values change continuously.

3. Description of the Existing Service

Figure 1 provides an overview of the Need To Share project. The underlying assumption of the Need To Share project is that a computable model of command intent is captured by the widely-used military abstraction of a "synchronization matrix" shown in the upper left of Figure 1 and associated map graphics which constrain unit movement. The entries in the synchronization matrix are descriptions of unit activities at different times (operational phases are matrix columns) and at different locations (unit components are matrix rows). The long range goal of the project is to value information at different nodes in a communication architecture based upon the relative utility of meeting command intent and to move information among nodes to increase the value of information available to make command and control decisions. The nodes of interest include nodes in a military command and control network, communication nodes used by local government and non- government agencies, and nodes used by other coalition partners in humanitarian assistance and COIN operations. For COIN operations in Afghanistan, a current barrier to achieving General Petreaus' information sharing goal of "understanding the people" is that information available in military networks and other associated government and non-government networks cannot cross information security barriers associated with the various networks. In the case of united States forces, even though government policy is that commanders at any level can declare a need to share information with government and non-government entities, current information system implementations do not provide support for

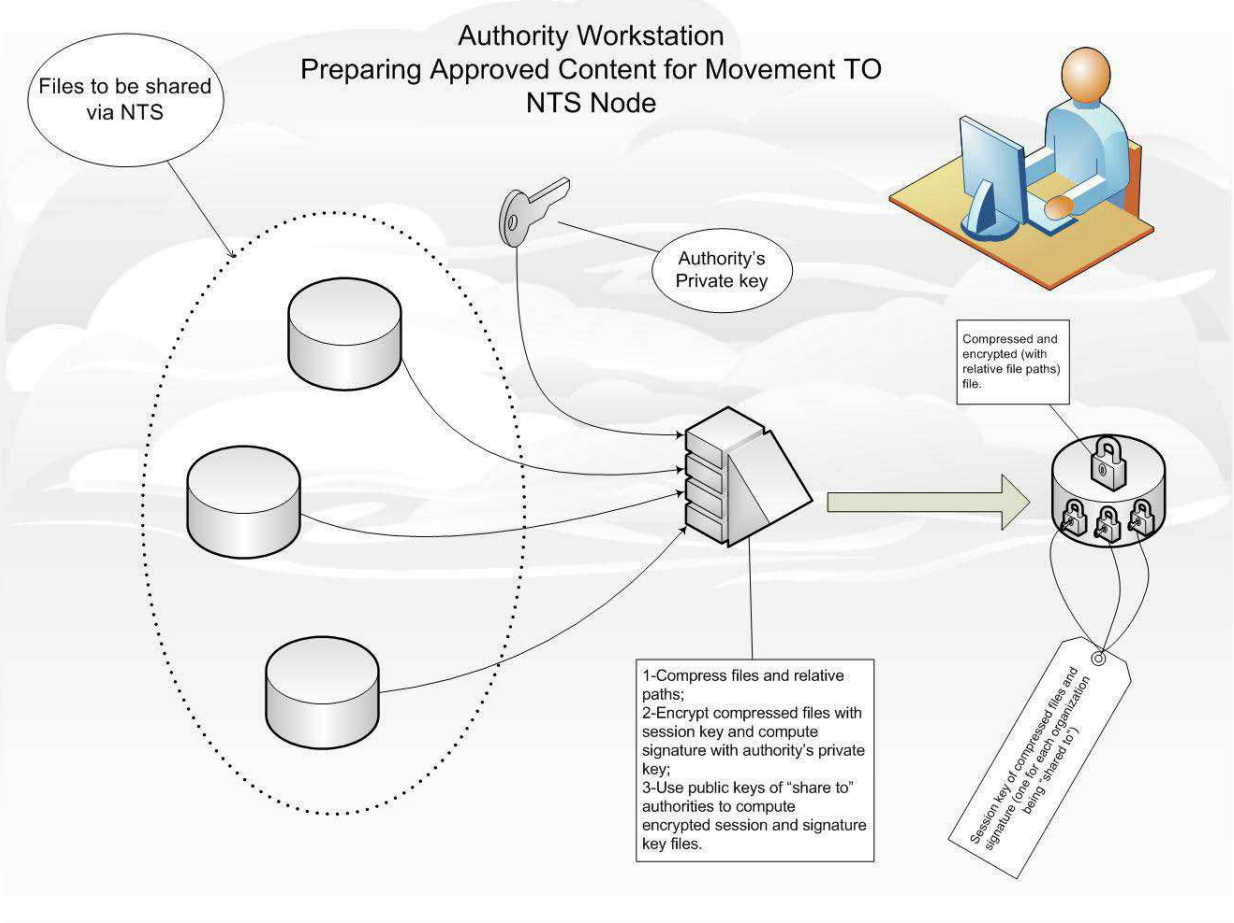

Figure 3. Preparing the data for sharing is achieved by a designated authority

automatically sharing information with entities who are not authorized to be "on the net" used by the military commander. As shown in Figure 1, our result provides a means for sharing information among nodes in a cloud-based communications architecture which, for military operations, can include nodes which are not "on the net" with other military units. Our initial implementation, described below, is moving sensitive but unclassified (SBU) information among nodes on the United States Defense Research and Engineering Network (DREN) and other communication nodes on the Internet. Figure 2 provides a summary of a representative process for selecting information to share.

Content placed in the repository is encrypted and signed. Only those groups "trusted" to have access to any specific set of data can open the encrypted form. When data is received in this manner, the first step in processing the data is to verify that the data was electronically signed by another group member. NTS member groups each have an "authority" who provides a public key that is available to each of the other authorities for encryption and authentication of NTS data. The repository can reside on a single commonly accessible node or be realized as a service accessed as a "cloud computing" service. FVI-NTS provides support for movement of static content (in the form of files and directory structure) with no "file type" constraints. The basic software supporting encryption and signing uses the OPENSSL software suite (the November 2009 version is FIPS 140-2 certified). Figure 3 provides a summary of the method implemented for encrypting the information to be shared with selected users and groups. The method depends upon implementation of some approach for generating and maintaining address lists and associated public and private keys for encrypting and decrypting the shared data. We refer to this as a Master Basic Trust Certifier (MBTC).

The FVI-NTS system follows a 5-step protocol for sharing information among clients in the cloud. These steps are request, aggregation, transport, decomposition, and consumption.

1) Request: When a user in an organization desires to share information (Figure 2), such as documents, media, data, etc, she must submit it to the organization's 'Authority' that analyzes the information and either approves are rejects the request. The 'Authority' (Figure 3) can be a person or an automated system.

2) Aggregation: When an outgoing set of files has been reviewed and accepted for sharing by the 'sending' organization's authority, the data is aggregated in preparation for transport. There are six sub-steps in the FVI-NTS protocol that accomplish this task.

1. The set of files to sent are compressed (including any relative sub-paths) into a ZIP file.
2. The ZIP file is encrypted with a randomly generated symmetric key.
3. For each node that files are being shared with, the symmetric key (generated in step 2) and the digest signature of the encrypted ZIP files are encrypted with the public key for the receiving authority. The file is then saved with the encrypted ZIP file (from step 2). The name of the encrypted key file is that of the node being "shared to." An encrypted key file is also generated for sending node (with its name).
4. For each node that is not being shared with, an encrypted key file is written but the symmetric key value used is zero (which never occurs otherwise).The set of files to be sent are compressed (including any relative sub-paths) into a ZIP file.
5. The set of encrypted key files and the ZIP files are saved to a directory named initially "Txxxxxxxxxxxx" where xxxxxxxxxxxx is replaced with the millisecond accurate clock on the authority's workstation.
6. After all the files have been copied to the local node, the directory is renamed with the initial "T" removed. [Note: only new directories without an initial 'T' are processed by receiving NTS authority workstations. Should an RSYNC capture a directory that has not been 'finalized' it will not be processed until a subsequent RSYNC occurs and renames the directory.]

3) Transport: After the files have been collected and encrypted, the authority the moves the set of files to the local node. At that point, the data is copied to the other nodes in the cloud (Figure 4). Each local node will have a directory of directories that acts as the repository of files to be sent or just received.

4) Decomposition of files to be shared with other members of the NTS group of organizations.

RSYNC will only copy new content to other nodes. All content on each node is encrypted. Each node has the needed keys to run RSYNC (within a SSH tunnel session) on each of the other nodes. No authority's private or public keys are ever stored on a node. Should a node's file contents ever become accessible to anyone outside the group of authorities participating in the 'need to share' group the content will remain 'secure' from inappropriate access. At the receiving end of the node cloud architecture, the tasks are the same, but simply reversed. The node authority will move the interested zip file (or files) off the node onto the local network.

5) Consumption: On the local network, the authority will use his public key to decrypt the ZIP file and proper disperse the files within his/her organization. Central to this design is the existence of a party acting as the Master Basic Trust Certifier (MBTC) that provides the access certificates on each node for the other nodes (thus allowing SSH-RSYNCH based communication). The MBTC also communicates the public keys of the authorities to each of the other authorities. The individual authorities for each organization can use OPENSSL software to generate their public and private keys. The MBTC does need to know the public or private keys of any of the authority workstations. What encrypted content the members choose to move is obscured from the view of the MBTC.

A specific MBTC can provide the management of the NTS group of nodes without ever having access to the actual content being transmitted. It should be noted that this architecture provides a solution to the end node problem, where an un-trusted, individual computer becomes part of a trusted, network. The data that is stored on each node is encrypted and essentially inaccessible to any node except for the intended receiver. As a result, there is no issue with a network -managed need to trust (i.e. the new end-node can only provide encrypted data to a network node which has chosen to accept the data from the new end node so some trust process has occurred and future trust activities can be among nodes can be monitored and controlled by the network controllers as desired). Any computer that joins the FVI-NTS cloud, however, must first obtain the proper keys from the MBTC.

4. Real-time extensions

While the work to date on FVI-NTS provides support for the trusted sharing of systems of files, it is strictly static in form. Operation of many

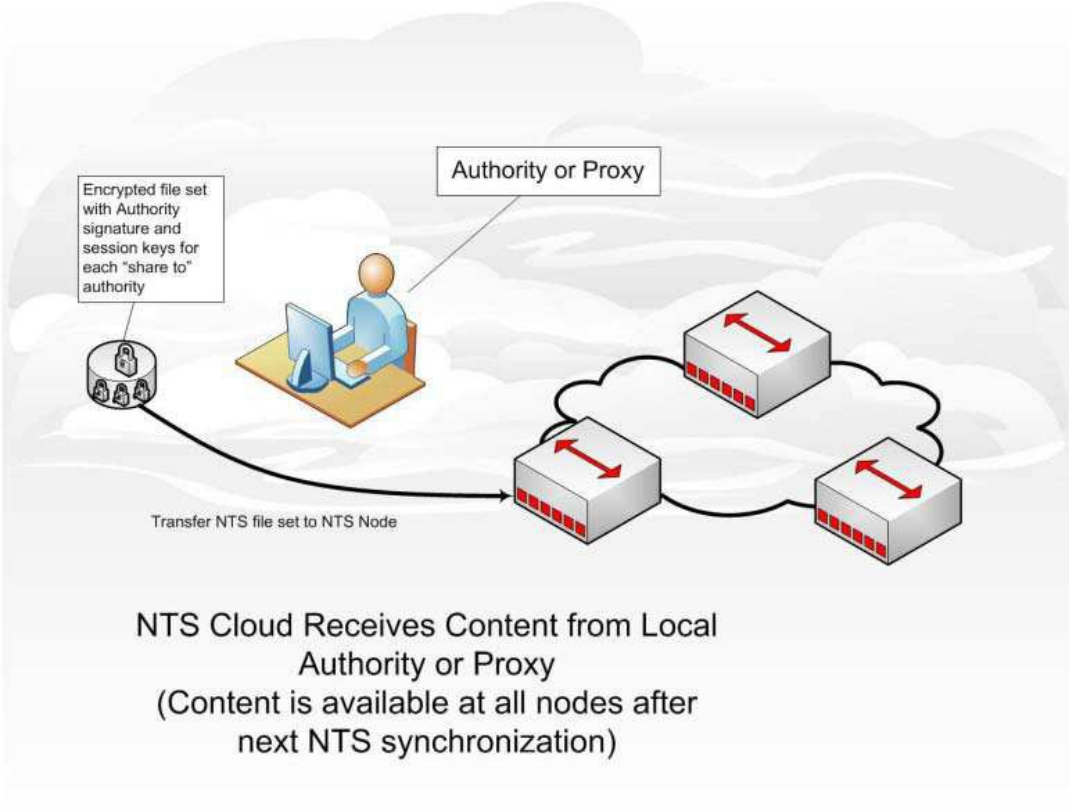

Figure 4. Sharing information among nodes in a communication network

systems generally necessitates the availability of real-time content (James and MCClain 1999, James and Mabry, 2004). Operation of many systems also frequently requires that information being transmitted be shared with only those trusted to receive it. For example, one challenge in enabling cooperative control of the smart grid in the United States is the requirement for an assumption of distrust among the operators of the various segments of the power grid in the United States (James , Dodge, Graham and St Leger , 2009) which played a minor role in the last cascading power failure in the United States and Canada.

Beginning with the concepts addressed in developing FVI-NTS, an additional operational form is being developed that supports need to share real-time streaming data. The same infrastructure concerns and guarantees are used to provide a service that allows multi-cast content to be shared from real-time sensing sensors or information sources in highly encrypted form for use by those "trusted" to receive it. The technical system supports segmented transmission of binary content that begins each segment with the encryption key for the following data transmitted in an encrypted manner using each trusted groups public key. Only members trusted to receive the content can decrypt a copy of the session key for the following segment. At the end of each segment sending group's private key is used to compute a signature for the preceding segment. This content is included in the encrypted portion of the segment. Any group receiving and decrypting the segment can then use the public key of the group sending the content to verify that there has been no modification of the content of the segment during transmission. Once a segment beginning is located the multi-cast content can be decrypted very quickly and its authenticity evaluated at the end of the segment. While the encryption overhead will be such to prohibit the sharing result in fast control loops present in telecommunications control and faster control loops, the sharing result will be usable in real- time decision support systems as well as in slower control loops such as chemical process control, water treatment facilities, or pipeline control systems. The length of the segment directly controls the maximum amount of data that may be received that could be tampered with before a trusted recipient would detect such tampering. Because the public keys are shared among the groups participating in the NTS partnership, there is no network based traffic to check credentials of the other parties. At the next received segment boundary any trusted member can begin decrypting the NTS-Real-Time (NTS-R) multi-cast stream. At present a fixed, pre-negotiated segment is used. Again, this avoids any additional network negotiation or transmission of information for what is a fixed body of service information and content.

In order to minimize overhead, member groups of an NTS partnership may be incorporated into one or more federations who are provided the same shared private key for those trusted to receive the content on the basis of federated membership. Only an individual group (not a federated set of groups) can provide an NTS-R source. Information being used to sense critical and sensitive information can be provided to any recipients trusted to receive the information. Any other party "listening" to an NTS-R stream can (at most) use the stream as a source of "white noise" but cannot determine any portion of the actual content included in any segment or the stream.

At each segment's start, a new decryption key is generated and then encrypted using the public key of each trusted group or federated set of groups, single public key. Note: the transmitting group may not be a member of one or more of the federated groups that they are providing content to. As such a transmitting node may not be able to decrypt its own transmission. The code is available for anyone interested in testing the current implementation, http:www.netscience.usma.edu.

5. Conclusion

We have described an extension and a formal result for a well-known information security result. These new results have enabled implementation of an approach for sharing protected information across security barriers in real-time. We have provided an overview of the mathematical underpinnings to the result as well as a discussion of an initial implementation of the approach for static information sets. We have described the current extensions to the initial implementation which support real-time sharing of information to overcome existing barriers to construction of decision support and real-time control of large-scale distributed systems which require sharing of information among different control systems which are distributed in time and space. Such control systems occur repeatedly in coalition efforts for security activities in COIN operations as well as in cooperative control of large-scale distributed system such as power grids, transportation systems, and gas pipelines.

The service provides decision makers a means of securely and automatically sharing critical information across security barriers based upon declaration of sharing policies. The declaration and

implementation of information sharing policies based upon a need-to- share has been shown to be compatible with information protection policies based upon a need-to- know. Indeed, the implementation of the need-to- share service is based upon extending the mathematical foundations of need-to-know information security systems.

6. Acknowledgements

The authors are indebted to the anonymous reviewers for many improvements in the paper. This paper is based upon work supported by the U.S. Army Research Office under Grant Award Number MIPR9FDATXR048. The views expressed in this report are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense..

7. References

[1] Aubin, J. P. (1991). Viability Theory. Cambridge, MA: Birkhauser Boston Inc.

[2] BAST, Board on Army Science and Technology. (2005). Network Science. Washington DC: National Academy Press.

[3] Bell, D. E. (2005). Looking Back at the Bell-La Padula Model. Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005) (pp. 337-351). IEEE Xplore.

[4] Bell, D. E., & LaPadula, L. (1973). Secure Computer Systems: Mathematical Foundations - Volume I. Mitre Technical Report 2547 .

[5] Denning, D. E. (1976). A lattice model of secure information flow. Communications of the ACM, Volume 19, Number 5, May 1976 , 236-243.

[6] Deshpande, A., & Varaiya, P. (1995). Viable Control of Hybrid Systems. In P. Antsaklis, W. Kohn, A. Nerode, & S. Sastry, Lecture Notes In Computer Science; Vol. 999, Hybrid Systems II (pp. 128-147). London, UK: Springer-Verlag.

[7] Foley, S. (1989). A model for secure information flow. Proceedings, 1989 Symposium on Security and Privacy (pp.
248-258). IEEE.

[8] Gong, L. (2009). Java Security: A Ten Year Retrospective. Proceedings, 2009 Annual Computer Security Applications Conference. Honolulu, HI: Conference Publishing Services.

[9] Honda, K., & Yoshida, N. (2007). A uniform type structure for secure information flow. ACM ACM Transactions on Programming Languages and Systems (TOPLAS), Volume 29, Issue 6 .

[10] Huggins, Kevin, Frank Mabry, and John James, "Flowing valued information based on a need to share," First IEEE International Workshop on Network Science, West Point, NY June 2011.

[11] James, J. R. (2000). Thoughts on Information Operation Detection as a Nonlinear, Mixed-Signal Identification Problem: A Control Systems View. Proceedings, 2000 IEEE Symposium on CACSD (p. 6). Anchorage, Alaska: IEEE.

[12] James, J. R., & Mabry, F. (2004). Building Trustworthy Systems: Guided State Estimation as a Feasible Approach for Interpretation, Decision and Action Based on Sensor Data. 37th Hawaii International Conference on System Science (p.
6). Kohola Coast, Hawaii: HICSS.

[13] James, J. R., & McClain, R. (1999). Tools and Techniques for Evaluating Control Architecture. Proceedings,10th IEEE International Symposium on CACSD (p. 6). Kohala Coast, Hawaii: IEEE.

[14] James, J., Dodge, R., Graham, J., & St. Leger, A. (2009). Gap Analysis for Survivable PCS: Final Report. I3P,
http://www.thei3p.org/publications/ResearchReport14.pdf.

[15] James, John R., Frank Mabry, Kevin Huggins, Michael Miller, Thomas Cook, Florian Tamang, Sam Abbott- McCune, Howard Taylor and William J. Adams. Secure Computer Systems: Extensions to the Bell-La Padula Model. West Point, NY: USMA Network Science Center. December,
2009

[16] Lanahan, Justin T., Allen Latty and Rodravian Murray, "Need To Share - Flowing Valued Information and Secure Networking," First IEEE International Workshop on Network Science, West Point, NY June 2011.

[17] Landwehr, C. E., Heitmeyer, C. L., & Mclean, J. (1984). A Security Model for Military Message Systems. ACM Transactions on Computer Systems, Vol. 2, No. 3, August 1984 , 198-222.

[18] Lee, E. A., & Varaiya, P. (2000). Introducing Signals and Systems, The Berkeley Approiach. First Signal Processing Education Workshop. SPE.

[19] Lee, E., & Varaiya, P. (2002). Structure and Interpretation of Signals and Systems. Addison-Wesley.

[20] Lygeros, J., Pappas, G., & Sastry, S. (1999). An Introduction to Hybrid System Modeling, Analysis and

Control. Preprints of the First Nonlinear Control Network Pedagogical School, (pp. 307-329). Athens, Greece.

[21] McLean, J. (1990). Security Models and Information Flow. 1990 IEEE Symposium on Security and Privacy. Oakland, IEEE Press.

[22] Ross, R., Katzke, S., Johnson, A., Swanson, M., & Stoneburner, G. (2008). NIST SP800-39, Managing Risk from Information Systems An Organizational Perspective. Gaithersberg, MD: NIST, http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd- sz.pdf.

[23] Ross, R., Swanson, M., Stoneburner, G., Katzke, S., & Johnson, A. (2004). Guide for the Security Certification and Accreditation of Federal Information Systems. Gaithersberg, MD: NIST Special Publication 800-37, http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf.

[24] Thompson, K. R. (2006). "GENERAL SYSTEM" DEFINED FOR PREDICTIVE TECHNOLOGIES OF A-GSBT (AXIOMATIC-GENERAL SYSTEMS BEHAVIORAL THEORY). IIGSS Academic Publisher: Scientific Inquiry, vol. 7, No. 1, 10.

[25] Tse, S., & Zdancewic, S. (2007). Run-Time Principals in Information-Flow Type Systems. ACM Transactions on Programming Languages and Systems, Vol. 30,No. 1,