Flowing Valued Information Based on a Need to Share

Kevin Hugins, Frank Mabry and John James
Department of Electrical Engineering and Computer Science
US Military Academy
West Point, NY, USA
{kevin.huggins, frank.mabry, john.james}@usma.edu

***Abstract*—The ability to share information between organizations in an ad-hoc, networked environment frequently found in humanitarian assistance/disaster relief (HADR) operations, remains a challenge today. For example, US Armed Forces participating in HADR operations do not have an organic ability to share information bi-directionally with Non-Government Agencies (NGO) such as Doctors-Without-Borders. It such cases, communications are normally accomplished outside existing military networks.**

There are several factors that contribute to these communication barriers. Information systems often do not respect the diversity of data that needs to be shared. Security protocols enforced between organizations are also a common challenge as trust policies do not support any ad-hoc 'extension' of an organization's network based on a "need to share" condition.

We present a solution that addresses these challenges. The Flowing Valued Information (FVI) Need-To-Share (NTS) architecture is designed specifically for organizations that need to share information with others in an ad-hoc environment. FVI-NTS supports a cloud computing architecture and provides an alternative approach to the *end node* problem in cloud computing. The design addresses authentication, authorization, integrity, confidentiality and non-repudiation—all within an ad-hoc environment and is based on open source code that has been FIPS-140-2 certified.

Keywords-Cloud computing, Distributed information systems, Computer network security, Network services.

I. INTRODUCTION

Networked, complex, and dynamic operational environments have become the norm for the US military. Where once traditional military messages were designed to support conventional military operations within the Army, present operations require more than just a flexible form for the content. Individuals and organizations that Army units must communicate with have changed greatly. These non-traditional parties engaged in communication may be coalition members, Non-government Organizations (NGO), or even local civilian leaders. The environment that the Army now operates in introduces new challenges that include (1) communicating with non-traditional parties (2) via non-military channels and (3) providing those portions of available information that they need and they are approved to have.

In the following section we provide a context of our current work and in section III we present research that is related to our work. We will then use section IV to present the NTS architecture and then discuss the design's security aspects in section V. After considering future work opportunities in section VI, we will conclude in section VII.

II. BACKGROUND

The need-to-share cloud-based solution is one of the components of the Flowing Valued Information (FVI) system. FVI seeks to enhance the flow of information on the battlefield by providing a framework for moving information to whom the commander declares has a need to receive as well as valuing information.

In particular, w e propose a three component design shown in Figure 1 below that includes a supporting adaptive communications architecture that we will discuss in detail in section III that enables the commander to manage information flow for his/her unit. The other two components leverage this communications architecture. In particular, we seek to implement a computable model of the commander's intent which will be used in conjunction with automatically value information, the third component of our solution.

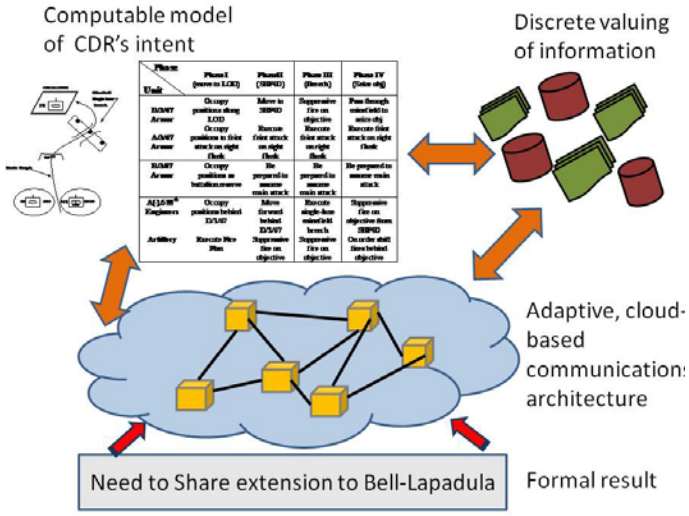

Figure 1. FVI major components.

Our approach has been to work from the bottom-up, addressing the foundational communications architecture first. We saw this aspect to FVI crucial to the success of the other features. As there was very little science to support a security model that accounted for the dynamic need to share information that is prevalent in many situations that the military finds itself, we started there.

One of the first results our group achieved was a set of extensions to the Bell-LaPadula model. We summarize our results here, but a complete discussion is found in [1].

Many of the available solutions for sharing information have successfully created multi-level secure systems (networks of systems) which follow access control rules (many based on the Bell-LaPadula security model) in which access to information is granted to a given level of classified information once confirmation is achieved that a given subject has the required clearance (mandatory access control). However, the current implementation of mandatory access controls and role-based access controls does not support mission success for those missions that require sharing information on an ad hoc basis, especially at the lowest tactical level for operations which require social and cultural awareness of local populations and NGOs as well as local support in achieving mission success.

Hence, we extended the Bell-LaPadula model to include continuous and discrete system states as is done for current general system theory for control of complex, distributed systems. We also extended the Bell-LaPadula definitions for "security" and "compromise" to include a definition of a “need-to-share” and a “failure to share”. A basic result concerning security in computer systems, using the precise notions for "security", "compromise", “sharing”, “need-to-know”, and “need-to-share” was then provided.

These extensions laid the groundwork for building more accurate models of the complex operational environments of today and tomorrow. Additionally, they provided the foundation for providing automation support for a commander’s decision to share information while simultaneously maintaining the security of information which must not be compromised. We then applied general systems theory to prove that a computer system with its data protected under a “need-to-know” policy could securely coexist with data managed with a “need-to-share” policy.

III. Related Work

There has been a lot of interest lately in efficient means for sharing information. In [2], the authors present a taxonomy of influences on intelligence information sharing that includes consideration of technical, legal and social elements. Our work is focused on addressing the technical barriers that they described. Several models assume or require a more permanent network architecture, e.g. [3], [4], [5] and [6]. Our approach is specifically designed for ad hoc, non-permanent networks. In addition, our approach enables fine-grained sharing of information in accordance with information sharing policy decisions made by the owners of the information (i.e. for military operations, unit commanders are the “owners” of information describing details of unit operations).

In [7] the authors present a taxonomy of Mobile Ad hoc Networks (MANETs). They separate them into two general categories: fully self-organized and authority based. FVI-NTS falls into the second category dividing their authority into two entities-authority and master base trust certifier (discussed below)—which enables secure and obscured transmission of data between nodes. There has been much work at securing the transmission layer protocols, e.g. [8], [9], [10] and [11]. Our effort is focused at the application layer and assumes that lower layers are secured.

IV. The FVI-NTS Architecture

The FVI-NTS node architecture (Figure 2) is an implementation of the formal results described in section II,

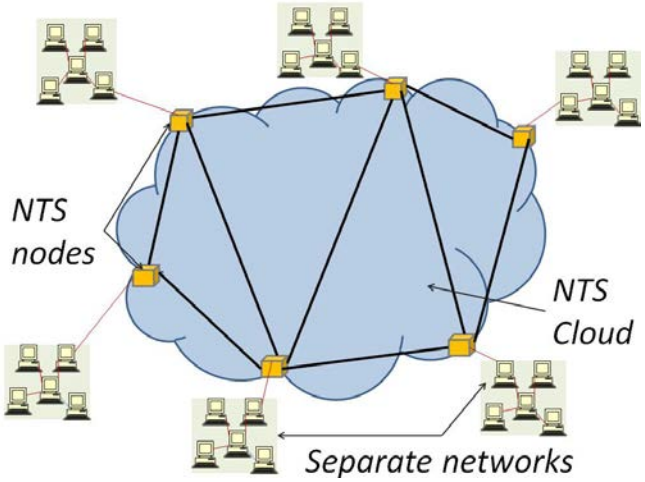

Figure 2. FVI-NTS cloud and attached networks.

above. It is an approach to provide automation support for a commander’s decision to share information with other organizations that may not be on the secure military network. The FVI-NTS solution does not alter any existing information security controls based on established “need to know” policies for maintaining information security. It should be noted that this architecture is specifically designed for information sharing in ad hoc networks.

A. Design philosophy

There are several assumptions and decisions that form our design philosophy. We list them here to provide a common foundation.

First, the FVI-NTS architecture makes no assumptions about the process results in a decision to share information by a local organization. This is outside the FVI-NTS system boundary.

Second, trust between the authorities that are the representatives for their respective organizations on the NTS group is the basis for sharing. No assumption about the actual distribution of information at the other end of a need to share relationship is ‘enforced’ by this software.

Next, how and with whom a receiving authority chooses to share contents from another organization is also not dictated by the system’s design. Agreement between authorities may result in ways of designating the parties in the receiving

organization information is intended for [additional files might be provided in the set of files being transmitted].

It should also be noted that the NTS design is not intended as a support for systems that require a "dynamic" response relationship. The nature of the file sets being exchanged is static. A session-based communications protocol, such as the Common Object Request Broker Architecture (CORBA), would not be appropriate in this design. Because the parties involved often do not have continuous, predictable network support, the design provides for allowing graceful operation and the ability to "catch-up" with operational results that occurred when a system experienced some network interruption.

Only the 'local' authority for each node accesses a node. Between the nodes, regular RSYNC executions occur that keep each sending-nodes' locally generated content files available on the other nodes. The actual transmission of content from the 'sending' node to the other nodes is controlled by the execution of RSYNC from a 'receiving' node

Finally, any complete replacement of the set of files associated with an individual transaction will be detected by the failure to decrypt the individual authority key for the ZIP file or the signature value also included with the encrypted symmetric key will not match the locally computed signature for the ZIP file.

B. Node communications protocol

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*. We will describe the FVI-NTS architecture in terms of these five steps.

1) Request

When a user in an organization desires to share information (Figure 3), 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. We make no assumptions and consider this part of the protocol outside the responsibility of FVI-NTS.

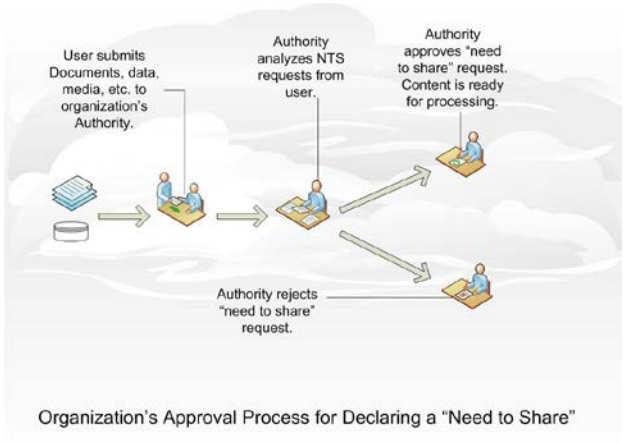

Figure 3. A user requesting to share information.

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(Figure 4). 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 "Txxxxxxxxxxxxx" where xxxxxxxxxxxxx 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.]

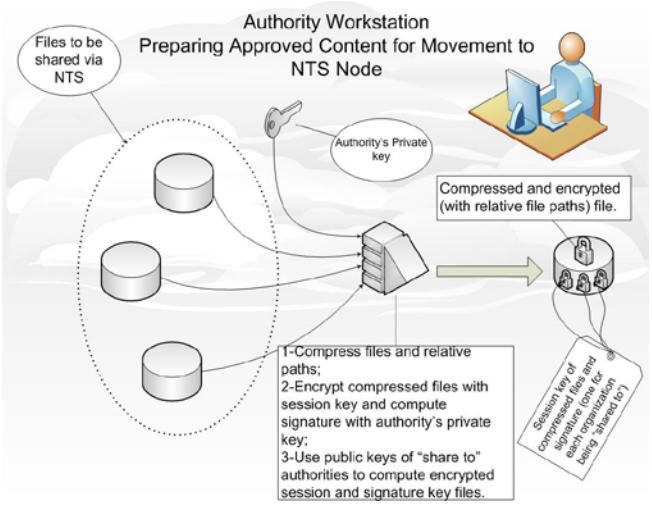

Figure 4. Authority workstation preparing documents to share.

Authority' can be a person or an automated system. We make not assumptions and consider this part of the protocol outside the responsibility of FVI-NTS.

3) Transport

After the files have been collected and encrypted, the authority the moves the set of files to the local node (Figure 5). At that point, the data is copied to the other nodes in the cloud.

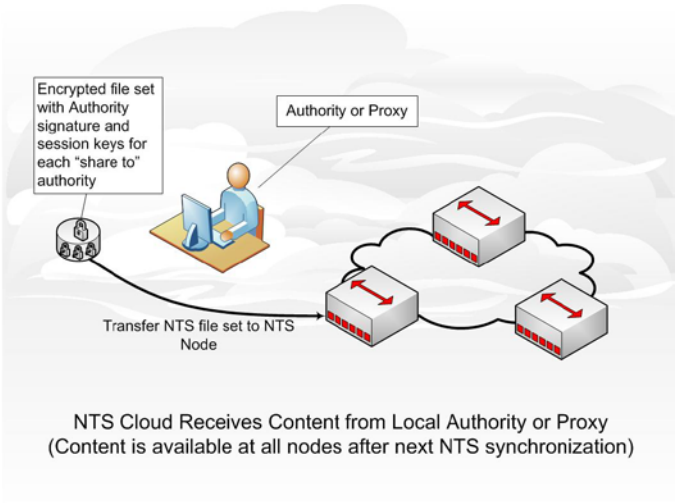

Figure 5. The Authority moves the collected files to the local NTS node.

Each local node will have a directory of directories that include the sets of sets[1] 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.

4) Decomposition

At 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 need to trust. Any computer that joins the FVI-NTS cloud, however, must first obtain the proper keys from the MBTC.

V. SECURITY

We now discuss the security aspects that have been designed into the FVI-NTS architecture. We will explain them in terms in terms of authentication, authorization, integrity, confidentiality and non-repudiation.

A. Authentication

The authority workstation operator is the principal individual of concern in NTS operations. He has access to a specific authority's private key which is needed to digitally sign content being approved for "need to share" from the authority's organization to select NTS member organizations. Movement of content between NTS nodes uses credentials loaded on the node by the MBTC. This data does not provide the information needed to decrypt any of the content being shared.

B. Authorization

What a specific NTS authority is limited to in the operations associated with the local NTS node is set by the design of NTD. What the authority workstation can access on internal files systems is outside any operational impact of NTS.

C. Integrity

The design of NTS provides for detection of any attempt to modify content after it leaves the authority workstation that provided the content to be shared. The encrypted ZIP file of the files being shared has a signature and symmetric session key provided to each organization's authority. Each receiving authority has the public key from the signing authority. This provides the means to computationally assert the integrity of the received transmission.

D. Confidentiality

This security aspect is addressed by the use of encryption of the actual data as well as the signature for the content by the originator. A symmetric key and cryptographic key are generated for every set of files being shared.

E. Non-repudiation

The present design provides for non-repudiation by the sender because only the sharing authority can sign the content (using the authority's private key). No specific provision

[1] This is not a typographical error. We refer to sets of files within other files such as folders within folders.

directly provides a secure confirmation of the receipt of the content by the designated recipients. If this functionality is needed, the receiving authority can simply "package" the transactional name of set of files received (after the receiving authority has distributed the files internally in the receiving organization) and "share" this information for response to the sending node and authority.

VI. FUTURE WORK

After extensive local testing, we plan to apply FVI-NTS in an operational environment using mission related data to demonstrate its capability to be used as a cross domain solution for information sharing. Our intent is to leverage our relationship with the National Military Academy of Afghanistan (NMAA) to move more sensitive but unclassified data between USMA and NMAA.

We are also currently working on applying FVIT-NTS with other network edge devices. We are initially using Android smart phones in conjunction with tactical robots as a proof of concept demonstration.

Finally, we are planning to develop a real-time extension called FVI-NTS-RT (real time). Using a multicast protocol, the goal will be to share streaming data, such as videos, in addition to static data.

VII. CONCLUSION

In this work, we have presented an overview of the Flowing Valued Information-Need-To-Share project and the problem domain it addresses. Additionally, we discussed our approach and described the FVI-NTS system architecture as well as future directions.

REFERENCES

[1] James, J. R., Mabry, F., Huggins, K., Miller, M., Cook, T., Tamang, F., et al. (2009). Secure Computer Systems: Extensions to the Bell-La Padula Model. West Point, NY: USMA Network Science Center.

[2] Treglia, J. and Park, J., "Towards Trusted Information Sharing", Proceedings from the 15th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 28 June – 1 July 2009, Paris, France, pp. 45-52.

[3] Krishnan, R., Sandhu, R., Ni, J. and Winsborough, W., "Foundations For Group-Centric Secure Information Sharing Models", Proceedings of the 14th ACM symposium on Access control models and technologies, June 3-5, 2009, Stresa, Italy, pp. 115 – 124.

[4] Sandhu, R., Raganathan, K., and Zhang, X., "Secure information sharing enabled by Trusted Computing and PEI models", Proceedings of the 2006 ACM Symposium on Information, computer and communications security, March 21 - 23, 2006, Taipei, Taiwan, pp. 2 – 12.

[5] Vatrapu, R. and Suthers, D., "Cultural Influences in Collaborative Information Sharing and Organization", Proceedings of the 3rd ACM International Conference on Intercultural Collaboration, August 19–20, 2010, Copenhagen, Denmark, pp. 161 – 170.

[6] Pardo, T. and Jiang, Y., "Electronic governance and organizational transformation", Proceedings of the 1st international conference on Theory and practice of electronic governance, December 10 - 13, 2007, Macao SAR, China , pp. 99 – 107.

[7] Van Der Merwe, J., Dawoud, D., and McDonald, S."A Survey of Peer-to-Peer Key Management for Mobile Ad Hoc Networks." ACM Computing Surveys, Vol. 39, No. 1, April 2007.

[8] Scott, D., "Relying on Time Synchronization for Security in Ad Hoc Networks," 43rd Southest Conference, March 18-20, 2005 Kennesaw, GA. USA.

[9] Conti, M. et al, "The Smallville Effect: Social Ties Make Mobile Networks More Secure Against Node Capture Attack," MobiWac'10, October 17-18, 2010, Bodrum, Turkey.

[10] Luo, L. et al, "Self-organized Group Key Management for Ad hoc Networks," ASIACCS '06, March 21-24, 2006, Taipei, Taiwan.

[11] Tsar, W,. and Pai, H.,"A New Security for On-Demand Source Routing in Modbile Ad Hoc Networks," IWCMC'07, August 12-16, 2007, Honolulu, Hawaii, USA.