Need To Share

Flowing Valued Information and Secure Networking

Justin T. Lanahan

Dept. of Electrical Engineering and Computer Science

United States Military Academy (USMA)

West Point, NY USA

justin.lanahan@us.army.mil

Abstract—The Flowing Valued Information (FVI) and Need to Share (NTS) project addresses implementation and security issues that arise when multi-national, government and non-government organizations (NGOs), have a mission requirement to readily share information. Current control measures, specifically within the US Department of Defense (DOD), only share information on a “Need to Know” (NTK) basis. This often is restricted to a hierarchy of classifications amongst organizations who already have an established trust relationship. This and other primary systems currently in use are often not sufficient enough in a large number of cases militaries and NGOs are finding themselves in today. Present doctrine in military coalition environments allow commanders to declare a “need to share”, however, there is no automated method to ensure timeliness and efficiency in distributing information across all entities who have a need for it. These environments also pose an issue of trust in military-NGO scenarios. Similar problems are also found in humanitarian aid and disaster relief (HADR) operations. Even though the information being shared may often be represented the same by all organizations, the infrastructure and protocols for movement and communications rarely are. The FVI-NTS project provides an automated means for supporting organizational information sharing in a trusted manner. It allows organizational authorities to implement automated command policies while maintaining the integrity of the data being shared. FVI-NTS formally proves the coexistence of both NTK and NTS controls. It also provides users an elegant but effective graphical user interface for accessing the above system that can be readily be deployed across many organizations regardless of environment. This front-end functionality expands the domain of possible implementation of FVI-NTS to serve as the standard for future DOD NTS network policies and requirements as well as other organizational groups with similar needs. The software is open source and supports operation on multiple computing platforms simultaneously.

Keywords—need-to-share; need-to-know; secure networking; security models; information sharing; trust relationships; organization relationships; information flow; data integrity; complex networks; information value

I. INTRODUCTION

A. Background

The increase in technology and globalization is rapidly leading to a world where military and HADR operations are largely handled by multinational organizations. Each of these organizations has their own mission, infrastructure, data, operating procedures, and relationships. When they are

suddenly thrust into an ad-hoc environment where the mission critically relies on the quick, reliable exchange of information a breakdown often occurs. This collapse happens on many different levels that not only hurts the reputation of an organization but also leads to a potential failure in the mission where lives may be at risk.

The breakdown is caused by a serious overhead when processing classified information across security boundaries. Further, it is caused by the inability to transfer information due to the resources at hand and the constraints of the working environment. It is a breakdown that organizations can not readily adapt to due to their varying resources and infrastructures. Even if organizations could adapt to the environmental and structural constraints, the problem of requiring certain clearances for material access would still exist [4].

After organizations have established a means of communicating and sharing information however minimal it may be, the issue of valuing the information being processed then arises. This causes organizations to be both deprived of the information essential to their mission and overloaded with information that is of no value to them at the same time. The latter wastes time and uses up resources in processing the information to determine its usability. The former is caused by organizations lacking a clear picture and understanding into the mission and roles of other organizations at a fine level of detail. This of course is unfortunate but understandable when an organization is focusing on their mission at hand and their needs and not necessarily calculating what information would be appropriate to pass along to others [6].

B. Flowing Valued Information

As a mission unfolds, the amount of information being generated is exponential. Each bit is a tiny piece in an immense puzzle to meet the commander’s intent of the operation. The commander has critical information requirements that are often assigned to specific positions to acquire and inform the commander. Subordinate leaders have a need for information that pertains to their specific roles and missions.

In the midst of this, the information being gathered by one entity may not be the information it needs. Common practice in any organization both governmental and NGOs is to report all information to a centralized headquarters, but this is often where it stops. Subordinate leaders may request information from higher levels, but this only happens so long as the leader

knows what he does not know and knows what is needed. Currently there is no underlying science for automatically moving valued information from one network node to another in accordance with a commanders intent and mission requirements [5].

C. Current Methods of NTS implementation

Despite the technology available to organizations, the most common form of information sharing is still word of mouth. This is based on the personal trust relationships built between individuals and not necessarily organizations as a whole e.g. a platoon leader may trust sharing information about the movement of his platoon to a local afghan national policeman so they can coordinate route security, but he may not trust exposing that information to the whole of the police organization [7]. In terms of efficiency, the current technologies are simply too cumbersome when not all information may even exist in a digital format, or there may not exist an infrastructure for digital transmission. Leaders are also concerned about the implications of sharing information digitally, where it has the potential to spread well beyond the intended recipients, thus adding risk to the mission and to their personal careers [8].

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) [2]. 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 non-government agencies as well as local support in achieving mission success. Thus, there is a need to explicitly enable categories of information which can be labeled “need-to-share” [5].

D. Purpose

The purpose of the FVI-NTS project is to provide organizations an efficient means of flowing information between their internal structure and to external organizations intelligently and quickly. This will give leaders confidence and trust in the privacy and integrity of their information. Further, it will allow for them to implement necessary control measures based on time and space as it relates to the need to share and the necessity of the relationships formed. This will all take place through a web interface developed in this project, which can be served online or through local network servers. This interface allows a streamlined approach for users who need to request, process, and send information in an intuitive, easy manner while alleviating the current concerns and issues detailed in this paper.

II. RELATED WORK

A. Bell-LaPadula Security Model

The Bell-LaPadula (BLP) model is the most widely used security access control measure amongst government

organizations. It focuses on the confidentiality and controlled access of classified information [2]. Its functionality is often characterized as “no read up, no write down” meaning that a subject may not read any information of a higher security clearance than his, and that the subject may not write any information available at a lower clearance level. This method is inductively proven to be secure by a set of transitions moving from one secure state to another [1].

B. Biba Security Model

Like the BLP model, Biba is also a formal model for security access control measures. Biba differs from BLP in that it focuses on the shortcomings of ensuring integrity in the BLP model. It is characterized by “no read down, no write up” to mean that information at different security levels are protected because information from lower levels cannot be read, thus the focus remains on one’s own current level and one can only write information at his level of clearance or higher so as to not potentially compromise higher level information by writing it at a lower level [10].

C. The FVI-NTS Difference

FVI-NTS takes from both of the above models to ensure simultaneous confidentiality and integrity and extends both to add the appropriate measures to implement sharing. The problems with the BLP and Biba models is their rigidity and inability to change or account for situations where information must flow outside of an organization that does not use the same security model [11]. NTS handles these differences by establishing the complex network dynamics of trust relationships declared by an organization that may change over time and space [5].

III. METHODOLOGY

A. Need-To-Know and Need-To-Share

The FVI-NTS project relies on the formal mathematical proof in [5] that NTK and NTS can coexist in the same domain. This enables commanders to accomplish the mission utilizing both methods of transmitting and making data available without a loss in integrity of the data or the organization based on the policies defined and actively modified by the commander.

The theoretical results in [5] extend the long-standing BLP result for defining a security violation in terms of a failure to maintain security constraints based on NTK policies [2]. The new result defines a sharing violation in terms of a failure to maintain sharing constraints based on NTS policies. Thus, implementation of the new result is compatible with existing security controls based on the long-standing NTK policies. Also, since the implementation only provides an extension to automate support for DOD NTS policies and does not alter existing security controls, the approach enables simultaneous compatibility of the two policies for protecting information based on prior NTK policies while implementing sharing controls under NTS policies [13].

B. Establishing Trust Between Organizations

Organizations working in ad-hoc environments inherently do not want to trust each other. They know their relationship is only temporary and that they all come into the environment

with a different mission, intent and background. This however does not take away their need to interact and share information. By allowing authorities within the organization to define their own security sharing policies the process of FVI-NTS can begin to automatically take place ensuring that an organization does not have to release any more or any less than it wants to until the relationship and roles become more clearly established. FVI-NTS helps along this process by ensuring the security and confidentiality of information even once it has traveled to an external organization. Not only is trust an issue between two organizations who have declared a need to share between each other, it is also an issue between a sharing organization and the organization that is handling the transmission of its information. This often occurs in Government-NGO relationships when a private corporation or organization such as Red Crescent or Doctors Without Borders have a need to work side by side with local military commanders who have established the FVI-NTS network for use by the varying organizations. Red Crescent may have concerns about the militaries use of their data and the strength of the encryption being used. However, due to the Open Source nature and encryption methods used by NTS, any organization can validate the processes being used. Once trust in the system has been established then organizations can begin to trust one another and work more efficiently to accomplish the mission [5].

C. *Maintaining The Integrity of Data and the Organizations*

What allows FVI-NTS to be so flexible in implementation is the fact that organizations have access to the repository being used. With this come serious issues of risk and trust concerns of those sharing information across the repositories. FVI-NTS ensures the integrity of the data by means of the current access controls and also through a very strong 4096 bit encryption, which is FIPS 140-2 compliant. This ensures only the intended recipient can view the information and that if the repository were lost, stolen or compromised in any way, that the information residing on it would still be safe, and would be backed up somewhere else on the cloud of nodes at other organizations using FVI-NTS. Not only does the encryption protect the sender and receiver of information to ensure its privacy, it also protects the medium through which the information is traveling through. This ensures that if there is malicious code residing in any of the information being shared that it will not be executed on the machine linked to the repository because the machine simply cannot read the data with the encryption. In a cloud networking environment this is also critical given the risk of a quick spreading vulnerability should a malicious file make it into the network.

D. *Organization Infrastructure and NTS Implementation*

Because the environments that FVI-NTS will be used in will vary greatly depending on the situation, it is essential that organizations have maximum flexibility in choosing how their information will be stored and transported. This will mostly be dictated by whether or not the organization has internet connectivity. If so, there are a multitude of freely available, open source repositories that may be utilized and offer the necessary features like r-sync. If no internet connectivity is present then FVI-NTS also recognizes a means of sharing that may be as simple as members transferring information through

portable storage nodes and manually syncing the data themselves.

Members of an organization that have established a need to share may access these repositories through the FVI-NTS front-end portal to share information in a number of ways depending on the internal structure of the organization. The interface can be stood up as a web server or it could reside locally on a work station that is interfaced through a web browser. All that is required is that the FVI-NTS front end be pointed to the local repository being used for sharing.

Because the front-end user interface for accessing the FVI-NTS nodes and processing requests for sharing needs is Open Source, organizations may easily modify it to suit whatever their needs and environment dictate. This component of FVI-NTS adds to its robustness since predicting all the different scenarios which it will be used is simply impossible. Especially in ad-hoc situations, when organizations do not have the time to formally develop a new system to support their mission, FVI-NTS gives them adaptive capabilities to constantly change their network and infrastructure however their mission requires.

IV. METHODOLOGY OF TRANSMISSION PROCESS

A. *Master Base Trust Certifier (MBTC)*

A key concept in FVI-NTS is the existence of a MBTC who provides the public keys needed to encrypt and access information on each node. This also allows for SSH_RSYNCH communication between nodes. When an organization becomes a part of the FVI-NTS network they generate a pair of public and private keys. What encrypted content the organizations choose to move is unable to be read by the MBTC thus a MBTC can provide the management of the NTS cloud without actual being a member organization participating in the sharing [13].

B. *Authority Workstation for the Local Node*

FVI-NTS ensures security of data by restricting access to an organizations node only by the Authority appointed by the commander for that organization. Once an authority has placed information on a node, which is all that is necessary for the “sending” of files as RSYNC then ensures that the files are distributed amongst the other nodes in the cloud network. This happens on regular intervals and can be changed according to the needs of the commander so that information is always available when it needs to be available [13].

C. *Sending and Receiving of Information*

1) *MBTC and Keys*: Each local sharing authority has encryption keys provided by the MBTC and has a procedure for declaring a “need to share” selected information.

2) *Request to Send*: An Authority at a transmitting node receives a request to share information. The file(s) are then made available to the authority for review.

3) *Send*: The Authority at the transmitting node transfers the information to be shared to the local organizations node.

4) *Cloud RSYNC*: The NTS Cloud makes the information to be shared available to those users and groups designated by the sharing authority as authorized to receive the information. Organizations will maintain a snapshot of their node, and each

time an RSYNC is performed, the new snapshot will be compared to the old to see if new files have arrived.

5) *Receipt*: The Authority at a receiving node makes the information available to those users and groups authorized by the sharing authority to receive the information.

D. Preperation to Send Information

After a request to send information has been made, a local authority then reviews the files to confirm the appropriateness of sending them outside the organization. If the request is accepted then the following steps occur on the authority workstation of the 'sending' organization:

1) *Compression*: The set of files to be sent are compressed into a ZIP file maintaing folder hierarchy if present.

2) *Symmetric Key Encryption*: The ZIP file is encrypted with a randomly generated symmetric key.

3) *Public Key Encryption*: For each node that files are being shared with, the symmetric key (2) and the digest signature for the encrypted ZIP file is encrypted with the public key for the receiving authority and the file is saved with the encrypted ZIP file (from step 2). This public key can be found with the MBTC who labels the keys by organization name. An encrypted key file is also generated for 'sending' node (with its name) so the 'sending' node may recover its information later in the event of a loss.

4) *Anonymity of Enryption*: For each node that is not being shared with, an encrypted key file is written but the symmetric key value used is zero that way there is no inherent knowledge that can be ascertained about who is sending information to who on the cloud

Figure 1. Process of an Authority preparing information to be shared.

All content on each node is completely encrypted. Each node has the needed keys to run RSYNC within a SSH tunnel session. However, no organizations private or public keys are ever stored on a node. Should a node ever become lost or stolen and its file contents become accessible to anyone outside the NTS cloud of organizations, the content will remain secure from compromise and inappropriate access.

E. Cloud Network Specifications

1) *Authority Privileges*: Only an authority can access an NTS node. This can be done directly, through a proxy, or web interface.

2) *Request Implementation*:. An organization can chose to set up a portal for the submission of file sets to be moved by an authority over the the cloud network. This interface is provided by the FVI-NTS project.

3) *MBTC and Public Keys*: The MBTC for the NTS cloud provides the set of public keys for the authorities.

F. Recovery of Lost, Stolen, or Compromised Data

FVI-NTS functionality loss or data compromise at an organization node can occur through any three of the following events: (1) Loss of the stored data through loss of the network attached storage device (NAS), (2) Loss of the Authority Workstation associated with a given node, and/or (3) loss of the MBTC which provides the trust certification for sharing data. The continuity of operations and disaster recovery plan for each of these three events is executed as follows:

1) *Recovery of local FVI-NTS Node shared data*: Local shared data for an FVI-NTS Node is recovered from other FVI-NTS Nodes through use of the use of rsync then recomputing the symmetric key values to determine what information belongs to the organization that needs to be recovered.

2) *Recovery of local Authority Workstation functionality*: The configuration and local files necessary to restart an Authority Workstation are backed up daily or as often as an authority wishes.

3) *Recovery of the MBTC functionality*: The configuration and local files necessary to restart the MBTC are backed up daily. Certifications and pass phrases are stored at minimum two different physical locations under two separate organizations.

V. FUTURE WORK

Though researched in the realm of government operations and crisis environments, FVI-NTS could take on many of the same roles in civilian corporations where the same need to share exists. This can be seen in a corporations need to protect proprietary information while also allowing a means to share portions of it and other information for marketing purposes [9].

Unlike currently emplaced security models that posses very rigid structures, FVI-NTS seeks a robust, flexible means of handling the needs of organizations. With this, the main area for future advancement lies in improving dynamic capabilities of FVI-NTS

A. Dynamic Trust Relationships

Like personal relationships throughout life, organizations posses many of the same attributes in their interactions with each other. Specifically, trust may change with time and vary over the different environments organizations find themselves in, and the actions they are taking. It would be necessary for a more robust implementation of FVI-NTS to account for these changing relationships and accurately model or perhaps even

predict and inform the commander of their changing state. Metrics would also need to be added to value information to a certain extent based on these trust levels. Likewise, organizations could be rated on their trustworthiness over time by assessing the value and use of the information being exchanged between them.

This automated approach would of course never be able to fully approximate the intent and implications of actions taken by organizations and thus will always require a level of human input on these ratings.

B. Dynamics of Missions and the Commanders Intent

Another factor that is always changing in one form or another is the mission and commanders intent. Though they may never change drastically, they do change based on the inputs of new information and new events that occur. A more complete implementation of FVI-NTS would recognize these changes and revalue old information and begin flowing new information appropriately based on the current situation.

C. Assessing Intent and Valuing Information

An intelligent version of this information processing would also be able to rate events based on the volume of information flowing through the network and its content and inform the commander of a potential shift in the mission before he even recognizes it. Authorities transferring information could better tailor this through the use of metadata, allowing FVI-NTS to better discern the relationships between information, intent, mission and events.

D. The load balance of Information

Essential to the ultimate effectiveness of FVI-NTS and the organizations using it is the actual ease of use and value of information being transferred and processed by entities. If an organization does not have the resources or time to analyze an immense volume of information being transmitted then it simply will breakdown and default to a pre FVI-NTS system instead.

Future implementations of FVI-NTS should feature an intelligent way of prioritizing information through the help of metadata and even priority inputs from commanders so that it may be transmitted faster to organizations with a need for it. As with the dynamics of mission and intent, any changes in the value of information should also update existing information and reprocess if necessary.

VI. CONCLUSION

It has been shown that the FVI-NTS project provides solutions to the current problems of trust, security, and flowing valued information when organizations have a need to share in ad-hoc environments. It has also been proven in [5] that this project does not have to replace the existing systems, as it merely extends them allowing for fluid implementation across organizations with well established security controls and large existing repositories of information classified under legacy access control measures. This paper places the previous results in the context of the potential contribution to military operations and reports on the implementation of an interface which implements the formal security results in a user-friendly manner. Because FVI-NTS only extends existing security

models it was thus proven that there indeed is coexistence between NTK and NTS without a loss of confidentiality or integrity. Also provided are thoughts on future work because it is important to note that solving trust relationships and proving the security of information sharing is not enough alone to make the information being shared valuable and that will be the areas that become most vital to a commander in the operational sense whether he is dealing with his own organization or coalition partners.

All of these features combined make for a very fast, reliable means of establishing trust in sharing information when time and situation do not allow for the overhead of clearing organizations and processing information with the current methods.

VII. TOOLS

The tools used in the implementation of FVI-NTS were selected on the primary basis that they be Open Source and robust. One of the primary intents of the project is that there exists an element of trust between all interacting organizations to include the medium which the information is actually travelling as well. Being Open Source means that any organization can validate the means by which FVI-NTS is sharing their information thus proving that the organization providing the medium is not attempting any malicious acts during the process.

It is also equally important that the interface being used by organizations to share information be Open Source also so there are no inherent issues that arise with concerns of data logging. When organizations enter a trusted relationship with a need to share they will obtain the necessary tools through local storage sharing or online. FVI-NTS comes packaged in a readily deployable system that is platform independent.

A. OpenSSL

OpenSSL is an open source implementation of the Secure Socket Layer (SSL) protocol. It provides cryptographic functionality which will be used in the encryption of information being shared. Because FVI-NTS will largely be used by DOD and government organizations it is necessary that it is Federal Information Processing Standard (FIPS 140-2) compliant. OpenSSL is one of the only Open Source programs that maintain this compliance.

ACKNOWLEDGMENT

The Network Science Center at USMA to include the advisors for FVI-NTS have provided valuable insight and laid much of the groundwork driving the motivation for the practical implementation of this project. The resources to achieve this have been made available by the generous grant that supports the Network Science activity for the FVI project, which encompasses NTS. The Principal Investigator and Co Principal Investigator of this grant are Dr. Frank Mabry and Dr. John James respectively. Many thanks go to them along with the readers of this paper, and the professional encouragement and wisdom of COL Grant Jacoby, the Computer Science Course Director, and COL Edward Sobiesk, the Information Technology Course Director, at USMA.

REFERENCES

- [1] D. E. Bell, Looking Back at the Bell-La Padula Model. Proceedings of the 21st Annual Computer Security Applications Conference [ACSAC pp. 337-351, 2005]. IEEE Xplore.
- [2] D. E. Bell, and L. LaPadula, Secure Computer Systems: Mathematical Foundations - Volume I. Mitre Technical Report 2547, 1973.
- [3] D. E. Denning, "A lattice model of secure information flow," Communications of the ACM, Volumn 19, Number 5, pp. 236-243, May 1976.
- [4] S. Foley, A model for secure information flow. Proceedings, Symposium on Security and Privacy, pp. 248-258, IEEE. 1989.
- [5] J. R. James, F. Mabry, K. Huggins, M. Miller, T. Cook, F. Tamang, et al. Secure Computer Systems: Extensions to the Bell-La Padula Model. West Point, NY, 2009.
- [6] C. E. Landwehr, C. L. Heitmeyer, and J. Mclean, "A Security Model for Military Message Systems," ACM Transactions on Computer Systems, Vol. 2, No. 3, pp. 198-222, August 1984.
- [7] J. McLean, "Security Models and Information Flow," IEEE Symposium on Security and Privacy. Oakland, IEEE Press, 1990.
- [8] R. Ross, S. Katzke, A. Johnson, M. Swanson, and G. Stoneburner. 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>. 2008.
- [9] D. D. Clark and D. R. Wilson, "A Comparison of Commercial and Military Computer Security Policies," IEEE Proceedings of the Symposium on Research in Security and Privacy, Oakland, CA, IEEE Press, pp. 184-193, May 1987.
- [10] K. J. Biba, "Integrity Considerations for Secure Computer Systems", MTR-3153, The Mitre Corporation, April 1977.
- [11] D. Hanz, Computer Science Laboratory at SRI International, "Policy-Based Data Downgrading: Toward A Semantic Framework and Automated Tools to Balance Need-To-Protect and Need-To-Share Policies," IEEE International Symposium on Policies for Distributed Systems and Netowkrs, 2010.
- [12] C. E. Landwehr, "Formal Models for Computer Security," Code 7593, Naval Research Laboratory, Washington , D. C. Computing Surveys, Vol 13, No 3, September 1981.
- [13] J. R. James, F. Mabry, K. Huggins, "Request for Approval of an Interim Authority to Test (IATT) of the Flowing Valued Information (FVI) Node," 2010.