



By Dr. J. Bret Michael, Daniel R. Hestad, C. Martin Pedersen, and Leonard T. Gaines

# Incorporating the Human Element of Trust Into Information Systems Policy

Exploring discretionary and mandatory policy about trust in terms of the structure and mission of an organization.

**T**rust is an inherently subjective notion. As such, trust is difficult to define, convey, measure, or specify. The individualistic nature of trust makes it difficult to incorporate into policy that can be applied across an organization. Yet trust policies within an organization permeate doctrine and procedures. Unfortunately, within those policies, trust is rarely defined; it is implicitly stated and individually interpreted.

To incorporate trust into doctrine or policy, one must first be able to define trust in the context of the doctrine, determine how and to what it is to be applied, identify why trust is important within the context, determine who will determine trustworthiness, and determine a measurement for success. In this article, we introduce a model that incorporates trust at the level of policy.

## Computational Models of Trust

Trust between humans is a cognitive function. Computational models of trust emulate and predict the way a human assesses trust. Existent models of trust that have been reported in the literature represent attempts to assign metrics to trust-based relationships between humans and their computer-based proxies (e.g., intelligent agents). These models address the notion of trust in many different ways and their definitions and metrics vary significantly. Many different meanings and connotations of the term “trust” have been proposed. In fact, if one examines the many definitions, one might come to the conclusion that existing trust models are an amalgamation of different beliefs and ideas.

Developing models of trust for human interaction is difficult; it is even more challenging when dealing with information systems. People are much more comfortable evaluating trust that involves interpersonal interaction, because it is easier to apply personal experiences, perceptions, and personal observation. Trust involving information systems, especially in a distributed system, requires a different set of trust variables. More trust has to be placed in elements that are unknown to the user. Adding to the complexity is the fact that interpretations of trust can differ among computing bases, domains, and applications.

## Demand For Trusted Systems

The effective use of information technology and success in any organization requires trust, not only of the information communicated, but also among faceless communicators. Our belief in the validity of the complex and subtle messages we receive by telephone or electronic mail is conditioned on how well we know and trust the senders. In a sense, psychological bandwidth varies directly with the degree of trust between people. Trust cannot be decreed. The willingness to trust is a combination of values and evaluation, attitudes, and interests. National culture influences how and whom we trust. But within and across cultures, trust depends on whom we consider trustworthy and how well we create trust in others. [1]

Why are trustworthy distributed systems difficult to develop? Part of the problem is transitive trust. Transitive trust is where person A trusts person B. Person B trusts person C. However, that does not mean that person A trusts person C. In distributed systems, one entity does not have control over all of the various parts that make up the whole. The developer will never have direct control over the server operating system, router software or hardware, transmission medium, or database software that support the application schema. As a result, the user has to rely upon someone else to ensure that the various pieces are trustworthy. This problem is compounded when the distributed system pulls information from sources that are outside of the control of the developer.

## Trust and Distributed Information Systems

When an organization uses to some extent distributed information systems to support its decision-making processes, members of that organization should try to answer the following question: *How much trust can we place in these systems as face-to-face transactions become increasingly rare?*

Trust can be thought of in terms of faith or confidence. If a ladder looks wobbly, one is unlikely to trust it to hold one's weight. Now consider trusting the mechanisms for enforcing security policy on the Internet. If the Internet



mechanisms for enforcing authentication, authorization, privacy, integrity, and non-repudiation policy do not appear to be sufficiently strong to the users, then users may hesitate to use the Internet for conducting business. Trust can be lacking for reasons both real and perceived.

One of the reasons there is not a high level of trust in the Internet for conducting business is that people simply do not understand the enabling technology or how to correctly apply it.

There are many ways of describing trust, as indicated by the results of the literature surveys conducted by Hansen and Gaines. [2,3] For example Jøsang defines two types of trust; trust in humans and trust in systems. In terms of information security, trust in a system is the belief that it will resist malicious attack. Trust in a human is defined as the belief that the individual will behave according to a given policy or expectation, and will not act maliciously. [4, 5]

Trust in an individual computer can be established by a number of methods. The protocols used can be tested for compliance, the hardware components can be checked, and it can be measured against a trusted computing base (TCB). Trust can also be established by a set of evaluation criteria such as the Trusted Computer Security Evaluation Criteria (TCSEC), Information Technology Security Evaluation Criteria (ITSEC), and the Common Criteria. However, when dealing with a heterogeneous distributed computing environment such as the Internet, establishing trust is more difficult. The Internet has no trusted computing base. It is also not possible to test the trustworthiness of all of the hardware and software that, for example, a mobile agent might interact within such a system. As a result, some feel that the definition of trust is based on the belief that trust should only be placed in people, as they are the ultimate decision makers [6].

There are almost as many models of trust as there are definitions. Most of the models are similar in that they attempt to assign weighing factors to subjective variables. Jøsang developed a belief model and related calculus called subjective logic that assigns degrees of belief, disbelief, and uncertainty to opinions and utilizes logical operators to apply them to trust chains. [7] Most models are also similar in that they model trust from the perspective of a single individual. In this article we introduce a model of trust from an organizational perspective.

Neither a purely mandatory policy, nor a completely discretionary policy are sufficient in developing an operational model when one's organization is competing in today's highly competitive information domain. A hybrid, or synergistic policy that takes the most applicable qualities of both and applies them to an organization is required.

## The Discretionary-Mandatory (D-M) Model

The principles of the Discretionary-Mandatory (D-M) model [8, 9] for trust are defined as follows: Enable those at the lowest levels the freedom of making decisions based on their own unique situations; this is the discretionary aspect. At the same time, allow for direction and guidance from the upper levels of an organization in the form of mandatory policies, as well as a common set of rules and standards, which reflect the nature of the organization itself.

The D-M model is a synergistic organizational model which recognizes the value of over-arching management policies while at the same time understanding the need for distributed decision-making. The real value in the model is that it allows top-down, bottom-up, and lateral flow of information and trust while allowing decisions to be made at the lowest levels possible.

Mandatory policies are those rules and requirements written by either the central oversight or by a peer organization. Mandatory policies should be general in scope so as to not overly restrict the flexibility and adaptability of the organization. No policy can be written which covers all possible situations (see Figure 1 on page 6).

In this model, the system will enforce mandatory policies: it is not left to the user to decide which policies are discretionary and which are mandatory. Much like the system of state and federal laws in the United States, some laws apply to the entire country and some to individual states. It is not the citizen who decides which laws are relevant.

The need for mandatory policies is clear. In any organization, of any size, there should be a common set of goals and a common vision for where the organization is going. To further illustrate the need for a common mandatory policy, we have provided a simple diagram (see Figure 2 on page 7) to visually show the reader the importance of a common mandatory policy within one's own organization, or across multiple organizations. In our illustration, we use language as our example, where all nodes in a system must have a common understanding when policies overlap so all units can communicate. Mandatory policies are traditionally set in place by the senior leadership. The simplest explanation of this is to relate it to organizational behavior. One would not want the lowest level in an organization making decisions without guidance and leadership (see Figure 2 on page 7).

Allowing subordinate levels in an organization to develop their own methods of conducting their business, within an overarching framework, provides the flexibility and adaptability essential in the Information Age. The speed at which information is transmitted and processed requires senior leadership to forego total control and allow subcomponents of their company, even to the lowest levels, the ability and trust to make decisions.

Particularly in a large organization, such as the U.S. Department of Defense (DoD), one would not want to apply the exact same policy regarding trust on a geographic combat-

ant commander as you would the Naval Postgraduate School (NPS). The DoD is a complex organization, with many moving parts, each with multiple and diverse missions. Constricting each subcomponent into one set of policies is not the best strategy in today's fast-paced environments.

To further demonstrate the practical application of the D-M model, we have put together several examples to illustrate our D-M model. Our first example references urinalysis screening as applied to the U.S. Navy and its zero tolerance policy.

### Example: Zero Tolerance

The U.S. Navy has a zero tolerance policy for narcotics use. To detect violations, random urinalysis screening is conducted at each command. When a service member tests positive for illegal drugs, his case is sent to a review board to determine the legalities of the situation. The matter becomes somewhat subjective rather than objective due to differing legal interpretations of the scientific process of drug screening. So instead of having a true zero tolerance policy, the U.S. Navy allows each command some discretion depending on the extenuating circumstances of each case. The D-M model reinforces trust by providing guidance and standardization in the form of mandatory policies, but realizes the importance of flexibility in distributed decision-making in a case-by-case basis.

### Example: Software Maintenance

Consider the following scenario—

*The Program Manager of an information system at NAS Anywhere contracts with a local software development*

*company XYZ to add functionality to the information system. XYZ accepts the contract, but does not have the in-house expertise, so they subcontract with company ABC in a third world country. ABC has an employee with anti-military views and inserts malicious code into the software, which subsequently deletes important files.*

This is a situation where a mandatory policy should have over ruled a discretionary policy. If the government's mandatory policy that software maintenance cannot be performed by third world nationals had been adhered to, the information system would not have been compromised. The program manager would still have the discretion to contract with XYZ, so long as they did not subcontract to foreign workers.

### Example: Aircraft Carrier Battle Group

A Carrier Battle Group (CVBG) is able to conduct sustained operations while being spread out over thousands of miles. The communications connectivity via satellite links for voice and data as well as point-to-point communications offers multiple paths across which data may be transmitted; this allows tactical and operational commanders to have access to constantly updated information about time-sensitive situations.

On the other hand, it also affords an adversary multiple opportunities to present deceptive information to our vast array of sensors in order to create confusion or give us a false sense of security. The goal of the adversary here is to extend the observe-orient-decide-act (OODA) loop so as to obtain a tactical advantage over the CVBG.

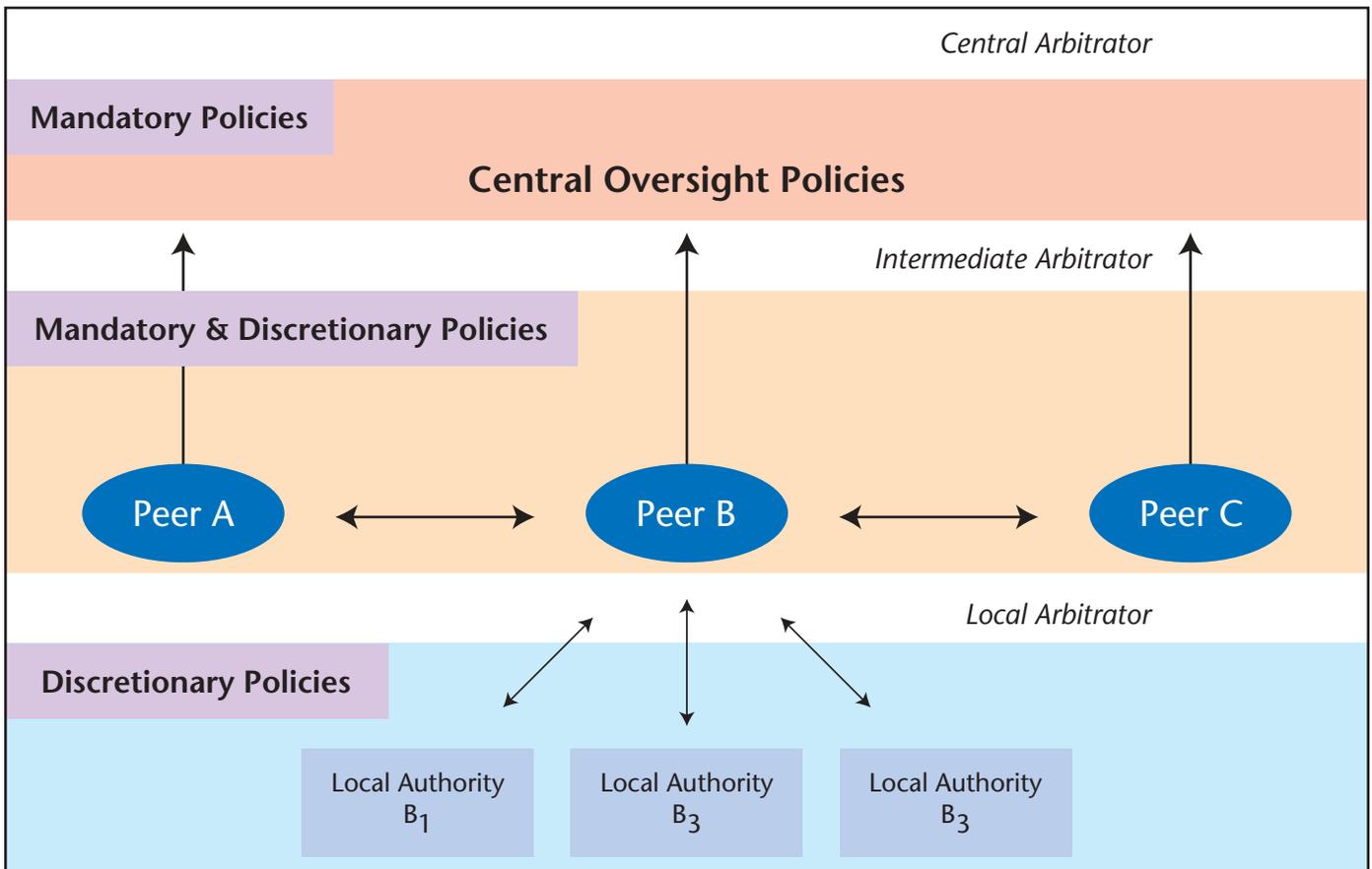
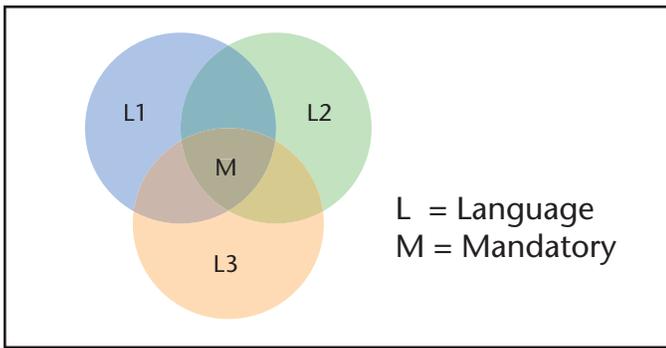


Figure 1. Discretionary-Mandatory Model



**Figure 2. Common Mandatory Policy**

When sensors acquire a contact, that information is transmitted to other platforms via a data link. It is also entered into a database to track over the long term. When the data on the contact is received by another platform, it appears on that platform's display in whatever symbology entered by the initial operator and classified by the contact's type (i.e., air, surface, or subsurface) as well as its relationship (i.e., friendly, unfriendly, or neutral). It is assumed that the contact was acquired, classified, and retransmitted correctly.

But this is not always the case. At each point, mistakes can be made. The contact could be a decoy designed to fool our sensors. The sensor operator could be newly trained and prone to error. In addition, the adversary, with the necessary transmitters and authentication procedures, could have inserted the data into the information system.

Moreover, it is not just an issue of receiving information and placing trust in that information, but also an issue of with whom are you willing to share that information. When the information is received from other organizations, issues of transitive trust must be addressed.

Consider the following scenario—

*A U.S. aircraft carrier is steaming in the Persian Gulf conducting normal flight operations. It has in company a U.S. Aegis cruiser along with an allied destroyer from nation X and an allied frigate from nation Y.*

*The allied frigate acquires radar contact on an unknown aircraft traveling inbound, which it classifies as hostile and transmits the track of the aircraft to the rest of the battle group. The frigate then loses radar contact with the aircraft but continues to update it as hostile in the shared database of the battle group.*

*The aircraft is then acquired by the Aegis cruiser at a distance of one hundred kilometers from the aircraft carrier. The Aegis system determines it is the same unidentified contact classified as hostile by the frigate. It is within the air-launched-weapons envelope of multiple theater threat aircraft.*

What should the Aegis cruiser do?

Although the U.S. Navy's doctrine and the standing rules of engagement would likely permit the Aegis cruiser to destroy the unknown aircraft, that would make little difference politically if the aircraft was a passenger jet. Alternatively, if the aircraft were hostile, then the Tactical Action Officer (TAO) would be held accountable for not engaging the aircraft.

The answer lies in how much the TAO trusts the information from the frigate. If there is an established relation-

ship over time, common procedures, and training to establish trust amongst the two platforms, then the TAO can act with confidence on the information provided. However, if there are no commonalities, or established trust relationships, then the trust assigned to the information will be lower. The TAO also needs to evaluate his trust in his combat team, his own sensors, and the combat systems information systems.

If the cruiser's radars are confirming the same information the frigate, then the TAO's trust in the information the frigate and his own systems are providing are going to be much greater. If the cruiser's radars provide conflicting information, the TAO's trust in the frigates information will be far less. The TAO may need to gather data from the destroyer before trusting the frigate's information.

Properly applied, the D-M model would account for the possible communication pitfalls in this scenario. Organizationally, the model would allow communication and procedural training to develop across platforms with no interference from a central authority, what we term "discretionary policies." This process would foster a more trusted relationship amongst the platforms. The model would also force the information systems to standardize their data integrity procedures by means of central oversight policies, which we term "mandatory policies."

The central oversight actor would be the operational commander, in this example the numbered fleet commander. He would promulgate mandatory policies to govern the actions of units in the operational theater. The peers would be the various tactical units involved in the operations: the aircraft carrier, the Aegis cruiser, the allied destroyer and the allied frigate. Local authorities would be the TAOs onboard the various units.

The fundamental concepts of the D-M model apply nicely to a dynamic, fast-paced and information-centric environment such as the battlefield. The model realizes the value of the input from the lowest levels; those who are directly involved in a situation and have the greatest need for accurate and precise information. At the same time, the model also allows for guidance, coordination and standardization from higher echelons in the organization. It also provides mechanisms for lateral communication inside an organization as well as communication across different organizations.

The D-M model is not reliant on a single input or piece of data and thus is insulated from single points of failure. It is easily applied to the short-term, single case decision-making situations. More importantly it applies to the long-term, strategic practices such as development of a Theatre Engagement Policy (TEP), foreign policy, economic policy; all of which, in their essence rely heavily on secure and trusted communications among many different countries, agencies, corporations, and people.

## Conclusion

There is always some degree of unpredictability associated with an information system due to misuse, lack of training, even general naiveté of the user. To construct systems with hard and fast mandatory security policies fails to recognize the human factors.

However, purely discretionary policy about trust is not the answer either. Such policy lacks the broad standardization to coordinate and share information outside the local domain. The answer appears to lie in an organized system that combines both discretionary and mandatory policies

to enforce agreed upon trust policy globally while permitting the human operators to use their discretion to evaluate the content of the information being shared at the local level.

There is ongoing research at the Naval Postgraduate School to further refine the D–M model. For instance, as part of his thesis research in the distance learning program in Software Engineering, Mr. George Walt of the Space and Naval Warfare Systems Center, San Diego, is exploring how to translate trust policy represented in the D–M model into system capabilities and requirements.

In addition, there is an ongoing collaboration between researchers at the Naval Postgraduate School and George Mason University to explore the technical feasibility of an approach for achieving adaptive system interoperability. In this approach, each local information system, within a system-of-systems, has a set of automated tools—known as a policy workbench—to aid in both the formulation and management of local policy. Returning to CVBG example, if the information-sharing policy for the shipboard command and control systems of nation X or Y changes, then the policy workbenches resident in the command and control systems of the Aegis cruiser could be used to query the policy interfaces of the systems of nations X and Y for such changes, reason about the changes, and update the local policy of the cruiser to maintain interoperability or some other property of the system-of-systems, including trustworthiness. ■

## References

1. Maccoby, M., Building trust is an art, *Research-Technology Management*, 40, 5, pp. 56–57, Oct. 1997.
2. Hansen, A. P., *Public key infrastructure (PKI) interoperability: A security services approach to support transfer of trust*, Master's thesis, Naval Postgraduate School, Monterey, CA, 1999.
3. Gaines, L. T., *Trust and its ramifications for the DoD public key infrastructure (PKI)*, Master's thesis, Naval Postgraduate School, Monterey, CA, 2000.
4. Jøsang, A., Trust-based decision making for electronic transactions, in *Proceedings of the Fourth Nordic Workshop on Secure IT Systems*, Stockholm University (Stockholm, Nov. 1999).
5. Jøsang, A., A subjective metric of authentication, in *Proceedings of the Fifth European Symposium on Research in Computer Security*, Springer-Verlag (Louvain-la-Neuve, Belgium, Sept. 1998), pp. 329–344.
6. Khare, R. and Rifkin, A. Weaving a web of trust. California Institute of Technology, 30 Nov. 1997; <http://www.cs.caltech.edu/~adam/local/trust.html>.
7. Jøsang, A. An algebra for assessing trust in certification chains, in *Proceedings of the Network and Distributed Systems Security Symposium*, The Internet Society (San Diego, CA, Feb. 1999).
8. Pedersen, C. M., *Trust and its ramifications for the DoD public key infrastructure*, Master's thesis, Naval Postgraduate School, Monterey, CA, 2001.
9. Hestad, D. R., *A discretionary-mandatory model as applied to network-centric warfare and information operations*, Master's thesis, Naval Postgraduate School, Monterey, CA, 2001.

## About the Authors

### Dr. J. Bret Michael

Dr. Michael has been an Associate Professor of Computer Science at the Naval Postgraduate School since 1998. His research on information assurance and information operations covers many aspects of distributed computing. Dr. Michael is a member of the IATAC Steering Committee. He may be reached at [bmichael@nps.navy.mil](mailto:bmichael@nps.navy.mil).

### LT Daniel R. Hestad, U.S. Navy

LT Hestad is a recent graduate of the Naval Postgraduate School's program in Information Systems and Operations. LT Hestad may be reached at [drhestad@empire.eclipse.ncsc.mil](mailto:drhestad@empire.eclipse.ncsc.mil).

### LT C. Martin Pedersen, U.S. Navy

LT Pedersen is a recent graduate of the Naval Postgraduate School's program in Information Systems and Operations. He is currently with the U.S. Space Command, Colorado Springs, Colorado. LT Pedersen may be reached at [martin.pedersen@peterson.af.mil](mailto:martin.pedersen@peterson.af.mil).

### LCDR Leonard T. Gaines, U.S. Navy

LCDR Gaines is a candidate in the doctoral program in Software Engineering at the Naval Postgraduate School. He is a graduate of the School's programs in both Computer Science and Information Technology Management. He is currently with the technical integration branch of the Naval Supply System Command, Mechanicsburg, Pennsylvania. LCDR Gaines may be reached at [Leonard\\_T\\_Gaines@navsup.navy.mil](mailto:Leonard_T_Gaines@navsup.navy.mil).