Security for the 22nd Century

Mark De Spain	Dr. John Darby	Dr. Robert Cloutier
Sandia National Laboratories	Sandia National Laboratories	Stevens Institute of Technology
P.O. Box 5800 MS0340	P.O. Box 5800 MS0757	
Albuquerque, NM 87185	Albuquerque, NM 87185	Hoboken, NJ 07030
U.S.A	U.S.A.	U.S.A
mjdespa@sandia.gov	jldarby@sandia.gov	Robert.Cloutier@stevens.edu

Abstract. Security in the 21st century is increasingly being characterized by rising asymmetric threats against long established and effectively monolithic institutions that are at the core of western infrastructure. The direction of technology development has the potential to further exacerbate the unbalanced standoff between the new threat and established institutions, whether government, commercial, industrial or cultural, particularly when the adversary is a determined and ideologically driven foe that is willing to bide their time and develop their resources over extended periods that may stretch into decades. Systems Engineering can offer security solutions that are not based on the traditional approach of adding layers of security to functional systems, but rather through the realization of inherent security that is implemented via the fundamental restructuring of organizational and product architectures that will "rebalance" the threat/risk equation and reduce potentially catastrophic asymmetric threats to a tolerable symmetric "standoff." Such restructuring does not come about easily or quickly, however, and fundamental shifts in infrastructure and culture can require generations to fully implement, so research into new security concepts today may not be completely realized until the 22nd century.

Introduction

Historical Perspective. In the 20th century, society, culture, industry, government, economics and power were consolidated into large, "economy of scale" organizational superstructures comprised of several intricately interwoven governmental, industrial and academic institutions. In the 21st century, these superstructures have critical points of vulnerability to a number of emerging security threats and technological obsolescence. The superstructure configuration was acceptable in an environment where large, monolithic adversarial structures, such as governments and industrial systems, faced off against one another; each party possessing complimentary strategic and tactical commitments to their own systems.

Today there are adversarial systems that have no comparable motivations or commitments to their respective systems, and motivational differences exist at many levels - including culture, philosophy and religion, politics and economics. These asymmetric cultural/societal/economic adversarial systems may explain why 20th century, monolithically structured systems now struggle against the "less" powerful yet more adaptable asymmetric threat structures.

Adjustments are needed to "rebalance" the opposing systems and achieve an acceptable risk/threat level. To accomplish this, enablers such as technology, are needed. However, technology is not a solution, in and of itself; rather the solution lies in *how* the enabler is applied. The issue with technology, as with most enablers, is that an established enterprise has a strong bias to apply technology in the same manner that it was applied in the past to solve similar

problems, both because of past success, and because humans "do best what they know best." Nonetheless, a well-implemented wrong solution is still wrong.

"Bunker" vs. "Distributed" Security. Many of the security systems found in the United States are designed to protect the superstructure against frontal attack – sometimes referred to as either the "bunker" approach or the "fort." Yet, they are struggling to fend off asymmetric security threats and competitive environments. The solution certainly does not lie in taking steps that will make the asymmetry even more pronounced, because asymmetry can be a significant contributor to security vulnerabilities and the cost to correct them. For example, typical bunker based security systems are based primarily on barriers that delay adversaries, and response systems that counter barrier breaches with armed force. They often require significant capital and lifecycle commitments that must be amortized over many years, and possibly decades, of use. However, rapidly advancing technology has the potential of rendering even the very best security technology of today, all but defenseless, against an adversary who is willing to wait until the right tools and technology are readily available. If asymmetry actually leads to inadequate security then the "right" response may be to reduce the asymmetry.

When the United States was in the midst of the infamous Cold War with the Soviet Union, the one factor that characterized both systems was an extensive social, commercial and infrastructures, containing significant proprietary information content. Their respective infrastructures defined them as entities, and it was the potential for each system to *symmetrically* threaten each other's infrastructure that, in part, enabled the virtual "stalemate" that existed for forty years. Today the West has real and potential adversaries that do not have the same commitment to the preservation of their infrastructure that is demonstrated by western society. The consequence of this value impedance is that the monolithic system structures are asymmetrically vulnerable.

It does not seem likely that most monolithic systems, especially infrastructure, can be realistically reduced to the same level of non-commitment enjoyed by the asymmetric adversary. However, that is where an enabler, such as technology, could make a difference. The proper application of a technology can enable the threatened system to become more symmetrical to the opposing systems rather than more asymmetric.

In practical terms, the reduction of vulnerabilities depends on many factors. These include the type of system (infrastructure, movable asset, process, data, personnel, etc.), the number and accessibility of significant targets, and the prudent application of technology and engineered architectures that enhance security. In order to use technology to reduce vulnerabilities, system based principles are needed that can be applied to a variety of threatened systems to transform them from asymmetrically appealing targets to symmetrically uninteresting non-sequiturs.

The alternative to the "bunker" approach to security may in fact be a distributed approach. There are a number of examples of distributed security systems in which one may find clues to enable the necessary transformation. One such system is the Internet. This distributed large-scale system has demonstrated robustness to various attack scenarios. While individual web sites or nodes have been rendered inoperable, there has yet to be an attack that has brought down the entire Internet. One reason is that there is no single controlling locus for the Internet - there is no "there" there. The Internet is a dispersed, non-centralized enterprise, both physically and operationally, that was originally devised, in part, to enable secure communication even in the event of nuclear war. While such a structure is not feasible for all systems, certainly the

security of many currently vulnerable systems could be improved by applying these and related concepts, such as redundancy, a distributed knowledge base containing atomistic elements in diverse locals, and numerous links between related information. Such principles may form the basis for a "distributed" security architecture that derives its integrity from a distributed asset that doesn't actually exist as a complete unit until the moment an authorized user initiates a task with the asset as opposed to the integrity of the barriers surrounding the asset.

On the surface, it might appear that these characteristics would actually serve to elevate the security risk by making the asset more accessible. Yet, overall security can be enhanced if these features are combined with other principles. One such strategy may be the implementation of a data set, or physical asset that does not exist as a complete and functional entity until the time of use. In this case, each separate and individual component represents a significantly reduced risk compared to the fully assembled end product.

A vulnerability that does exist for the Internet and related systems, such as e-mail, are the numerous links that are the very lifeblood of their operations. In this case, security can be improved by employing linking mechanisms that are dependent on ancillary information. Examples of possible sets of ancillary information include: time or place of use; specific user involved; special encoding required to access or assemble the dispersed elements; and other indicators of an authorized user or application. Some of these techniques are already being applied by financial institutions, such as credit card companies, which employ sophisticated monitoring programs to analyze usage patterns in order to identify possible unauthorized use.

Developing Security Solutions

Architecture, the Key to Distributed Security. The careful reader will noted from the previous discussion that the primary characteristic of a "distributed" security system has far less to do with the security itself and far more to do with the structure or "architecture" of the asset. That is, what is actually being distributed in space, time and use is the asset rather than the security. The required security is then molded to the needs of the distributed asset. The implementation of distributed security not only requires a re-thinking of what is meant by security, but may also include a complete reconfiguration of the asset, its lifecycle, ancillary support functions, tasks and hardware, as well as all related processes. Compared with typical product development, such a dramatic change in product development and lifecycle support requires a complete restructuring, not just of the product, but also of the organization producing the product. For this reason, and because there is such a fundamental connection between lifecycle, architecture and distributed security, it may not be practical to adapt legacy systems to a distributed security implementation.

Implementation of distributed security requires a high degree of coordination between design and logistics. In fact, logistics becomes as much a part of the design as any element of the product, because, in essence, system integration and product "final assembly" does not occur until the time and place of product use, and preferably, the elements of the product are not even co-located until that time. These objectives may be readily achievable when dealing with purely intellectual property, such as data, software applications and process information, which can delivered via networks, however, the problem is compounded when dealing with physical assets, and it is further complicated if significant elements of the system involve personnel.

People represent a unique challenge, but there are organizations that have adapted certain operational principles that fit nicely into the notion of distributed security, specifically, terror cells, and Marine and Special Forces units. These organizations use models that do not invest

critical skills or knowledge in single individuals, but broadly distribute roles and capabilities to insure unit effectiveness, even if that cannot be assured at the individual level. With respect to operational or mission knowledge, it is common practice to strictly segregate mission critical information to ensure any single compromise does not jeopardize the overall mission effectiveness.

In most cases however, there seems to be some element of the system, whether intellectual property, real property or certain select personnel, which could unduly damage the overall system if acquired or otherwise compromised by an adversary. So every system requires at least one and possibly several "keystone" elements that are unique and crucial to the function of the rest of the system. This may be a key piece of data, a software routine, a hardware component that is not easily duplicated, or an individual with essential information. These keystone elements require special attention and options to ensure system security. In the case of intellectual and real property, the proper response may be to ensure the destruction of the element rather than risk that unit falling into the possession of an adversary.

Of course, self destruction in response to a breach of security brings its own difficulties; specifically, an adversary may be completely satisfied with the outcome of a system that will destroy its most valuable asset by merely "tweaking" the security perimeter. Therefore, the integrity and function of the security system is fundamentally dependent on information that will reveal the "intent" of the adversary and the potential for the system to neutralize the adversary prior to taking such dramatic action as destroying the asset. With today's modern analytical capabilities, certain simulations could be employed to develop Concept of Operations (CONOPS) and related Command and Control (C2) options that will identify those "conditions of attack" scenarios that most strongly suggest that the destruction of the asset is the favored option for assuring that an adversary does not obtain operational control of a critical element. Some scenarios exist in which there is actually an advantage in not having to secure all elements of the system at the same level of security. First and most obvious, there is the judicious use of resources. Security that does not have to be applied in one place may be applied at another, more critical point, with greater effect.

Finally, another consideration, which is considerably less obvious, but perhaps even more significant, is that a great deal of useful information on an adversary's intent and capability can be acquired by surreptitiously monitoring the security state of less critical elements of the system. If the system is architected to gather intelligence on an adversary's attempts to neutralize security measures and attack the system, then there is greater opportunity to develop a more effective response when the time comes to neutralize the adversary.

Objectives of Bunker based Security Systems. There are common objectives of security, whether "distributed" or "bunker" based, and they go well beyond the obvious goals of protecting a high valued asset and enabling the authorized access and use of that asset. The other, more subtle and perhaps even more important goals of security, as discussed in the previous section, have more to do with understanding the adversary than protecting the asset. Whether explicitly acknowledged or not, understanding the motivation, objectives and capabilities of an adversary is an inherent element in any security system. The issue, of course, is that the developer and operator of a security system may not have a clear picture regarding who is the adversary. With the changing face of international and corporate relationships, this is particularly true for a "bunker" based security system that may have to be in placed for many decades. Under those conditions, the entire security environment and adversary mix can dramatically change.

Apart from thwarting an actual attack, the number one objective of security should be to reduce the value of the target in the mind of the adversary so that, ideally, an adversary would not even seriously consider mounting an actual attack. There are several ways this might be accomplished. The first may be through deception by making the asset appear to be something (less valuable) than it actually is. Another is to divert the attention of the adversary - maybe using a pre-emptive strike against a potential adversary who would then be busy protecting his own assets. Both of these have their place, but cannot be considered useful as a long term strategy. Deception has limited utility because it requires the keeping of secrets, and the history of secrets shows that they have a finite half life. While a useful tactic, diversion of attention also has its own limitations because it can involve significant resources that may not be available, at least in the long term.

"Bunker" based security seeks to lower the value of an asset from the viewpoint of an adversary by making it too "costly" for the adversary to access and possess the asset. But the bunker approach has negatives that adversely impact security as well. First, it can be costly to build and maintain a bunker, second, a bunker can actually complicate the authorized access and use of an asset, third, a large bunker infrastructure can easily give the impression of being impregnable – at least to the authorized user, even after a savvy adversary has found and exploited weak links in the security chain. The bunker also "points a finger" right to the asset and announces that there is something here of value to the bunker owner. Finally, it can become outdated and expensive to update to more modern threats. Bunker security designed even a few years ago may not have been designed for the flexibility and agility of the modern day threat.

Bunker security is driven by an inherent western attitude that equates "value" with possession and use of an asset, and relies on economic rights of ownership and successful task completion that are necessary for acquiring and using assets. Other societies may operate with different value systems that may not depend on "right of ownership" and successful task completion. These values could include aspects of "honor," religious zeal, political influence and even perceived notions of moral "right" and "wrong." The result is that the mere act of attacking a "bunker" oriented security system may bring its own reward, regardless of the "success" or "failure" of the endeavor.

Objectives of Distributed based Security Systems. Conversely, a security system that relies on a diffuse and distributed asset may present reduced barriers for an adversary to access some of the elements, and there is little to be gained for anyone who does acquire the element, whether judged in terms of actual, useable value or appraised by other less tangible measures such as psychological or political gain. Whereas bunker security lowers the value by raising the cost, distributed security reduces the actual value of the asset even if the adversary should gain possession of portions of the asset. An argument could be made that both approaches rely on the cost to the adversary of acquiring and using the asset. While there is some validity to this position, if architected to do so, there are other inherent advantages in a distributed security system. These include the information gained about the adversary, the options and response time available to address a security breach, the reduced threat due to a security failure, additional options regarding the asset lifecycle, a greater potential for security and product upgrades, adaptation to new security conditions and perhaps other advantages as well. The downside to the distributed approach is that being a new security concept there may well be vulnerabilities and costs not yet identified that will require time and experience to develop practical operating principles and implementations.

Three Elements of Security. Another objective of security is to acquire information about the adversary and enable the broadest range of response options. Information is the lifeblood of security and is essential for the correct execution of both distributed and bunker based security. A bunker has no security value if the defenders have no information regarding the breach location or the nature of the threat. The function of barriers in bunker security must be to both shield the asset and supply information (traditionally in the form of guards or "lookouts") in order to enable the defenders to make judicious and appropriate responses to any attack.

A case could be made that the main function of all security, regardless of the type, involves three elements. First is the acquisition of information on an adversary and the condition of the defenses. Second is to provide sufficient time for a defensive response to be developed which has the capability of neutralizing the adversary, and the final function of security is to neutralize the adversary and re-secure the system. To a first order then, differences in the types of security involve how information is gathered, the type of information acquired, the means of providing time for a response to develop, and the response options that are available.

In a bunker based security system, under full frontal attack by an adversary, there may be little time to gather and assess information. Under those conditions there may be few options available for response, with the potential that what response is made could over-compensate or under-compensate for the actual threat conditions. However, the nature and intent of a distributed security system that includes covert observation of less critical elements of the system is to enable sufficient time to monitor the actions and capabilities of an adversary in order to assess and prepare an appropriate response commensurate with the threat condition.

Another objective of security is to neutralize the insider threat, and, if implemented correctly, distributed security has an obvious advantage over bunker security when addressing the insider. With the bunker approach, the asset typically exists in a fully functional and usable state, and only requires the application of certain privileged knowledge to achieve an equivalent "authorized" level of functionality. While privileged knowledge can be compromised by various means, and significant resources are required to ensure the continued integrity of the "authorized" access information, quite often an asset can be compromised by an adversary with the right knowledge without having to resort to acquiring the authorized access information. In any case, the insider threat is particularly egregious, whether it involves acquiring privileged access information or otherwise understanding the means for compromising the "authorized" use of an asset.

Unlike a bunker based security system, in which the fully functional asset is vulnerable to someone possessing the right "key," the intent of the distributed security system is to disperse the asset physically and temporally – this includes the information that is needed to integrate the disparate elements into a functional whole. The objective is to achieve a condition where a conspiracy, involving several people that are widely separated with respect to responsibility, position and knowledge, would be necessary to compromise a distributed security system.

This approach, however, goes completely counter to what is normally required just to design, build, test and field a functional product. Implementation of a distributed security system will require the development of new systems engineering principles and methodologies in order to achieve a functional product without compromising the level of security provided by a distributed knowledge base.

The "Lean" Connection. One of the principles of distributed security is a "minimal" footprint in terms of both the asset and the supporting security system. An advantage of a reduced

footprint is that resources are minimized across the board. The astute reader may have observed that a distributed security system has many principles in common with "lean" production. The primary advantage of lean is the reduction of resources in the "pipeline" of the product stream lifecycle. By minimizing the capital invested in the product stream, a lean production enterprise can more readily adapt to changing environmental, technical and business conditions. In the same manner, a distributed security system can more readily adapt to changes in the environment due to technological advances available to both the adversary and the security developer, as well as changes in the motivation, capability or nature of potential adversaries.

Of course, there can be a downside to lean, whether applied to normal product lifecycle or a distributed security system. Specifically, the performance of the product, as well as the security system, is highly dependent on the reliability and accuracy of the supporting logistics. This was touched on briefly earlier in the paper, but any disruption to the flow of material and information can wreak havoc on both lean production and distributed security systems.

Analyzing Security Solutions

Analysis of Bunker and Distributed Security. While the forgoing discussion has been illuminating, difficult and potentially expensive decisions regarding the implementation of security, especially those that will affect product architecture, design and operation, will require careful and thorough analysis. Given the broad impact of security on a product or operation including design, logistics, operations, security force effectiveness, and production and lifecycle costs, no single analytic tool or perspective is sufficient to address the entire gamut of security. While a detailed analysis and comparison of bunker vs. distributed security will require future studies, the basis for an analysis can be addressed in the balance of this paper.

The analysis of security, like any other human driven and governed endeavor, is not readily and deterministically resolved by traditional, "hard" science techniques, but one methodology that may be useful in evaluating the value of various security architectures is "fuzzy" logic. A specific implementation of a fuzzy logic based analysis tool is "LinguisticBelief" that has been under development at Sandia National Laboratories.

LinguisticBelief is a computer tool for the evaluation of combinations of linguistic variables. Using the tool, linguistic variables are combined by approximate reasoning on fuzzy sets for the variables. The belief/plausibility measure of uncertainty is used to capture and propagate uncertainty for the linguistic variables. The tool is appropriate for the evaluation of variables that are difficult to express numerically. The belief/plausibility measure of uncertainty allows evaluation where there is significant epistemic uncertainty.

The mathematics of fuzzy sets, approximate reasoning, and belief/plausibility are complex. Without an automated tool, this complexity precludes their application to all but the simplest of problems. LinguisticBelief automates the use of these techniques, allowing complex problems to be easily evaluated.

When we use linguistics (words) to classify events, the words have a type of uncertainty called "vagueness." For example, yesterday was "sunny," public confidence in the stock market is "high," etc. Vagueness is uncertainty as to how to classify a known event. For example, assume we know how tall John is, but instead of saying John is 6 feet 2 inches tall we categorize John as "tall" without a precise definition of "tall." The linguistic (word) "tall' is vague. Vagueness can be addressed using the mathematics of fuzzy sets.

The belief/plausibility measure of uncertainty from the Dempster/Shafer Theory of Evidence is an extension of the probability measure of uncertainty that can better capture

epistemic uncertainty. Belief/plausibility is a superset of probability and under certain conditions, belief and plausibility both become probability. Under other conditions, belief/plausibility becomes necessity/possibility, respectively. Belief/plausibility addresses a type of uncertainty called "ambiguity." The uncertainty associated with predicting an event in the future is ambiguity.

A simple example illustrates the difference between aleatory (stochastic or "random") uncertainty and epistemic (state-of-knowledge) uncertainty, and the use of a belief/plausibility measure. Consider a fair coin, heads on one side, tails on the other, with each side equally likely. The uncertainty as to the outcome of a toss–heads or tails–is aleatory. The probability of heads is ½ and the probability of tails is ½. The uncertainty is due to the randomness of the toss. Suppose, however, that I do not know the coin is fair; the coin could be biased to come up heads, or the coin could even be two-tailed. Now that I have epistemic uncertainty, my state of knowledge is insufficient to assign a probability to heads or tails; all I can say is the likelihood of heads (or tails) is somewhere between 0 and 1. To consider epistemic uncertainty as well as aleatory uncertainty, belief/plausibility can be used as the measure of uncertainty. With total ignorance about the coin, the belief that the toss will be heads is 0 and the plausibility that the toss will be heads is 1; similarly, the belief that the toss will be tails is 0 and the plausibility that the toss will be tails is 1. Belief/plausibility forms an interval that can be interpreted as giving the lower and upper bound of probability. If I have enough information, both belief and plausibility reduce to a single value, probability. Epistemic uncertainty can be reduced with more information. If I toss the coin a few times and a heads and a tails occur, I know the coin is two-sided; with more tosses I can evaluate the fairness of the coin. Aleatory uncertainty cannot be reduced with more information.

While the operation of the program will not be described in this paper, the sighted reference provides a full explanation of the use and application of the program. The following figures illustrate the comparison of bunker vs. distributed security that was performed using LinguisticBelief. The reader should note that the inputs to the application are primarily notional, though a brief explanation of the rational used in the analysis is provided in the text.

The premise of the analysis is that security is measured by risk which is a function of the adversary threat, the vulnerability of the security system to attack, and the severity of the consequences if an adversary attack is successful. Before proceeding, the reader should note that there are several factors not included in this analysis. One, as noted above, is a defensible validation of the values used to generate the results, but other factors include, among others, those issues listed earlier, specifically product design, logistics, operations, security force effectiveness, and production and lifecycle costs.

Figure 1 provides the general structure of the analysis as applied to both the bunker and distributed security systems. There is not room in this paper to describe the full Linguistic Rules structure as applied to the threat, vulnerability, consequence and risk analysis factors. However the inputs used for each factor are provided below.

For the Adversary Threat factor the Basic Linguistics inputs included: Adversary Estimate of Damage, Adversary Capabilities Required, and Adversary Attack Preparation Required. The Vulnerability to Attack factor used two intermediate Rule Linguistics (see figure 1) since the total number of Basic Linguistics inputs (5) exceeded the allowed number of four inputs. However, for the purpose of this paper it is easier and completely legitimate to only list the Basic Linguistics that were used to derive this factor, which were: Defender Detect Capabilities Acquisition by Adversary, Defender Detect Adversary Attack Preparation, Defender

Disrupt Adversary during Capabilities Acquisition, Defender Disrupt Adversary during Attack Preparation, and Defender Defeat Attack. For the Consequence of a Successful Attack factor the Basic Linguistics inputs included: Adversary Estimate of Damage, and Defender Mitigation of Damage.

See Table 1 for the values of the Focal Elements developed from the fuzzy sets for the Basic Linguistics that are used in the analysis. The numerical differences in Table 1, for the bunker and distributed security systems, account for the differences in the results of the "Rule Linguistics" parameters of threat, vulnerability, consequence and risk. Note that a blank in table is the same as a zero. Also note that the values along a horizontal should add to one.

Figures 2a and 2b illustrate the possible threat to bunker and distributed security systems respectfully. Note that the lower the "threat" value, the better, which is also true for the other parameters of vulnerability, consequence and risk. While the differences in the results are not dramatic, there is a reduction of the overall adversary threat for the distributed system relative to the bunker system that is due primarily to a reduction in the damage that an adversary believes they could inflict by attacking a distributed security system. In other words, if the amount of damage an adversary can inflict is proportional to the adversary's access to and use of the intact asset, then a system in which the asset is physically distributed complicates the goal of the adversary in inflicting damage through access and use of the intact asset.

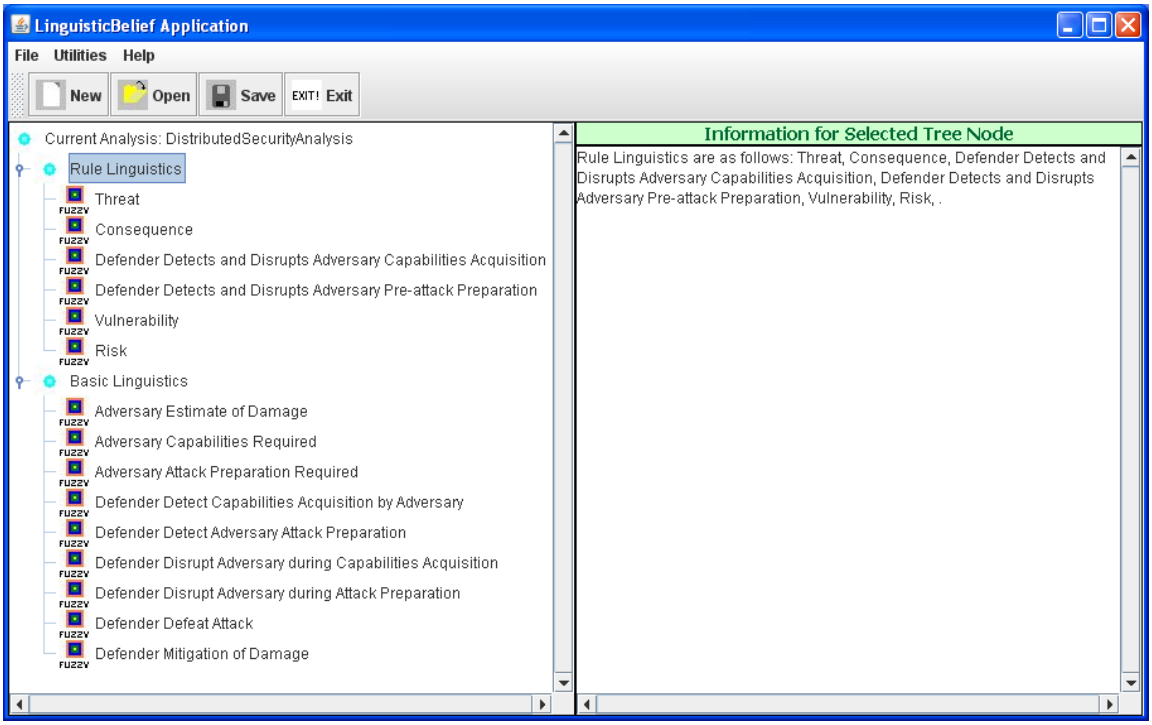

Figure 1. Structure of LinguisticBelief analysis of bunker and distributed security.

Table 1	Focal Elements of Fuzzy Sets for Basic Linguistics					
Adversary Estimate of Damage	**Negligable**	**Negligable & Low**	**Low & Moderate**	**Moderate & High**	**High & Very High**	**Very High**
Bunker	0.05	0.15	0.3	0.3	0.15	0.05
Distributed	0.1	0.2	0.4	0.25	0.04	0.01
Adversary Capabilities Required	**Low**	**Low & Medium**	**Medium**	**Medium & High**	**High**	
Bunker		0.5		0.5		
Distributed		0.4		0.5	0.1	
Adversary Attack Preparation Required						
Bunker		0.2		0.8		
Distributed		0.2		0.8		
Defender Detect Capabilities Acquisition						
Bunker	0.8		0.2			
Distributed	0.8		0.2			
Defender Detect Attack Preparation						
Bunker	0.5	0.3	0.1	0.05	0.05	
Distributed	0.5	0.3	0.1	0.05	0.05	
Defender Disrupts Capabilities Acquisition						
Bunker	0.8	0.1		0.1		
Distributed	0.8	0.1		0.1		
Defender Disrupts Attack Preparation						
Bunker		0.6	0.3	0.1		
Distributed		0.6	0.3	0.1		
Defender Defeat Attack						
Bunker		0.3	0.4	0.3		
Distributed	0.1	0.3		0.4	0.2	
Defender Mitigation of Damage						
Bunker	0.9	0.1				
Distributed	0.2	0.2	0.3	0.2	0.1	

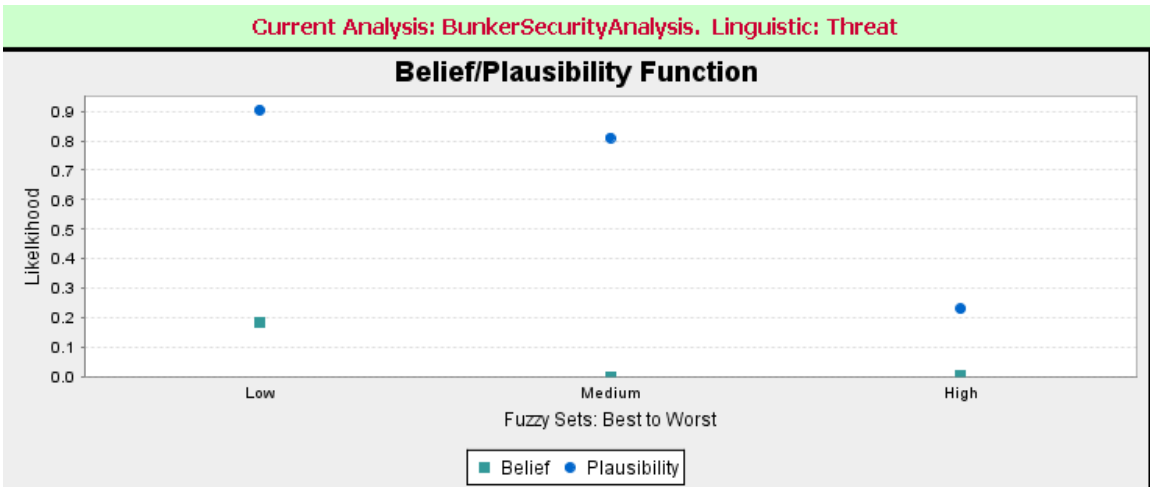

Figure 2a. The likelihood of a threat to a bunker security system.

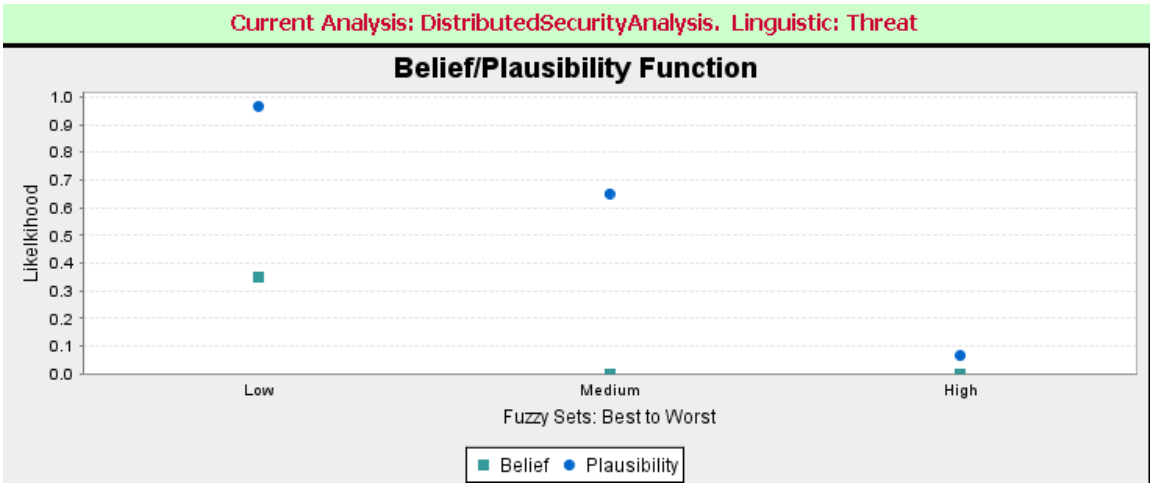

Figure 2b. The likelihood of a threat to a distributed security system

Figures 3a and 3b illustrate the vulnerability of the respective security architectures. The difference in the belief/plausibility function between the two systems is due to the greater likelihood of a defender defeating an attack on a distributed system since an adversary must successfully co-ordinate several operations either simultaneously or clandestinely over time to successfully achieve their attack objective. This effectively increases the likelihood that the security forces can interdict and neutralize at least on or several of the adversary operations. Note that the vulnerability of a distributed security system is bimodal while that of the bunker is monotonically increasing. Further analysis may be in order to confirm the legitimacy of these distributions.

Figures 4a and 4b illustrate the consequence of a successful attack on the two systems and Figures 5a and 5b illustrate the overall security risks based on the values of threat, vulnerability and consequence.

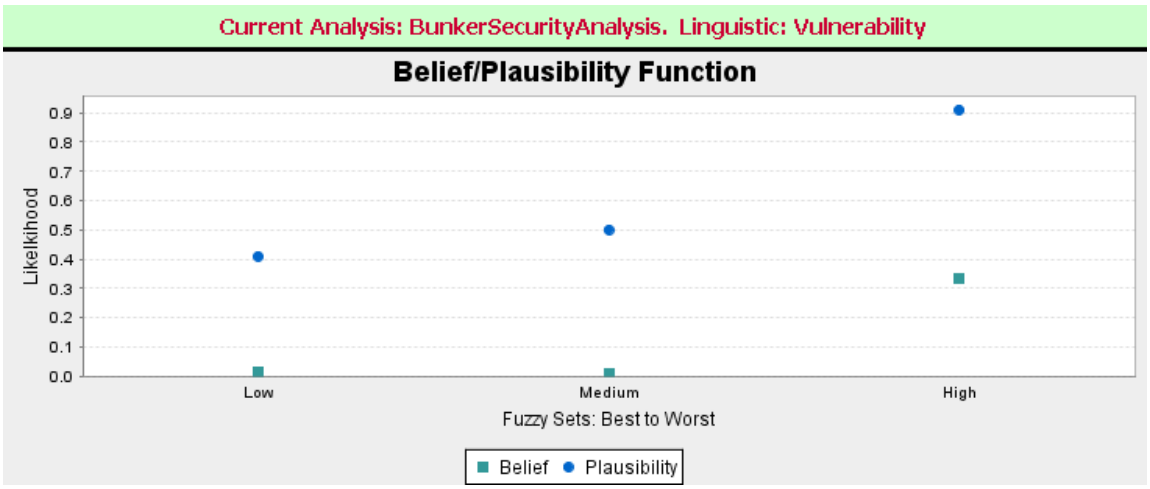

Figure 3a. Vulnerability to attack of a bunker security system.

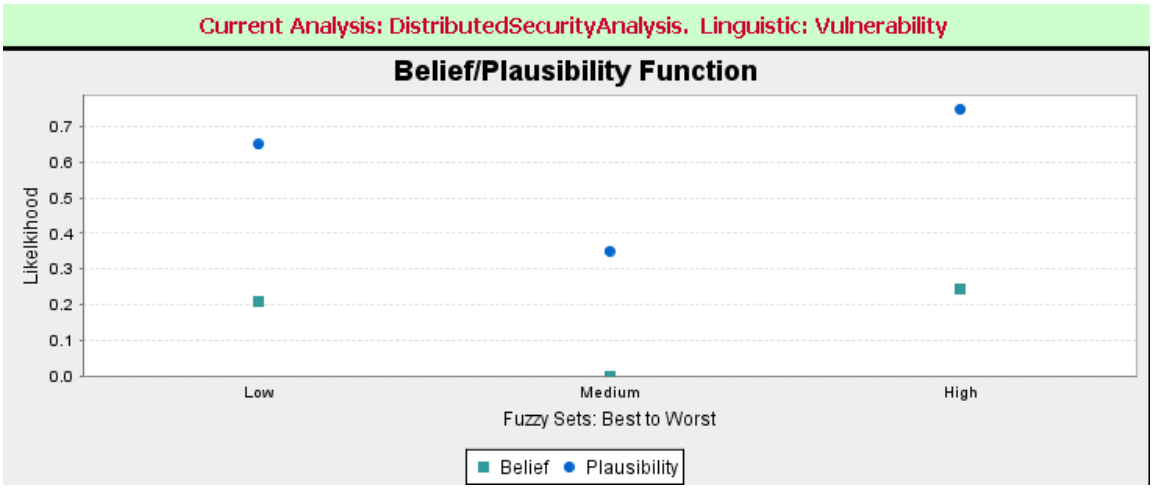

Figure 3b. Vulnerability to attack of a distributed security system.

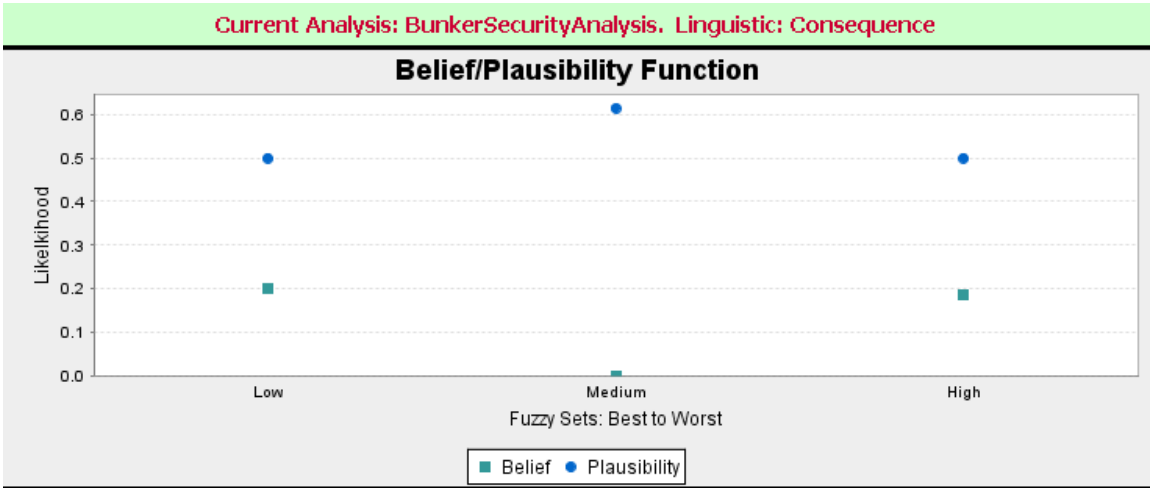

Figure 4a. Consequence of successful attack on a bunker security system.

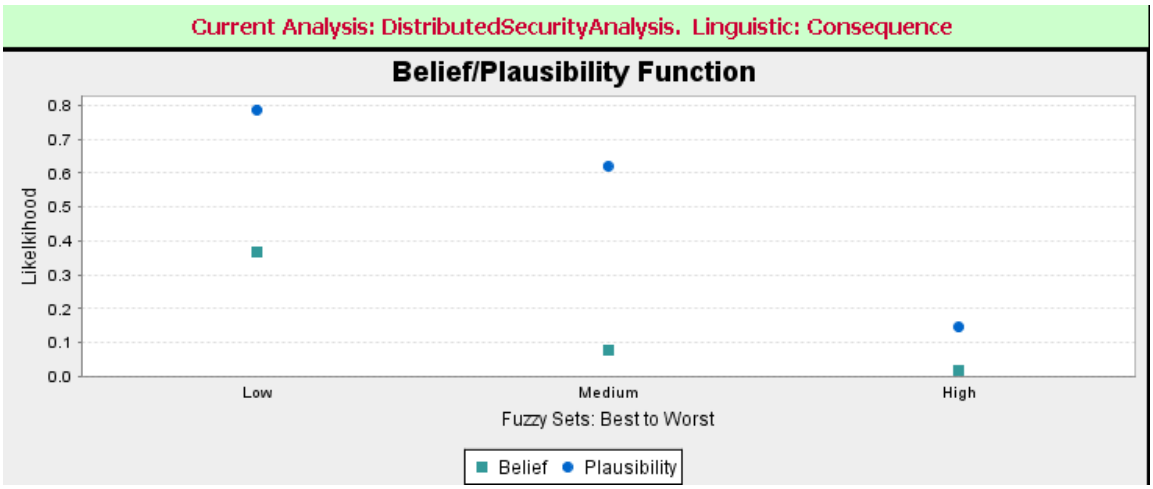

Figure 4b. Consequence of a successful attack on a distributed security system.

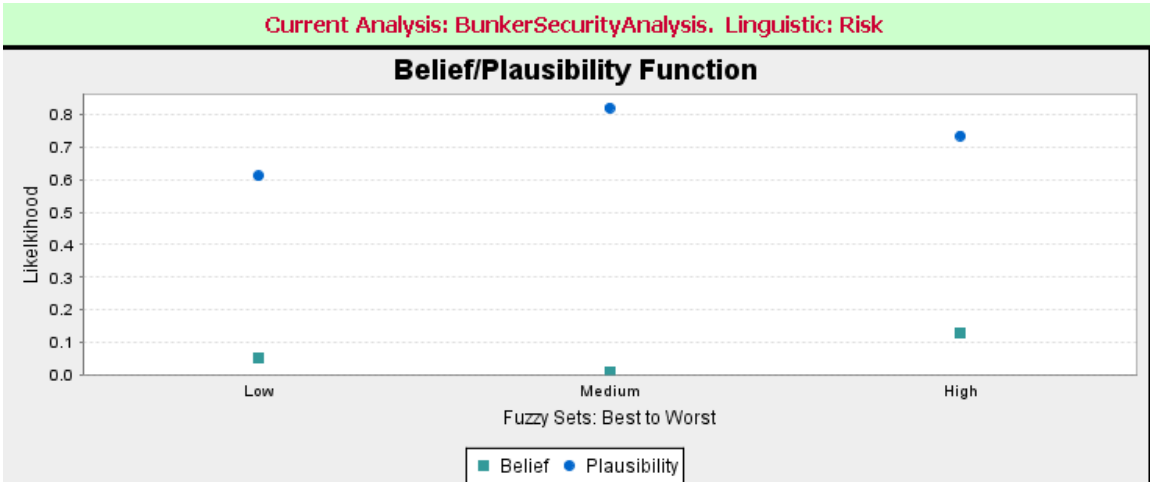

Figure 5a. Risk of an adversary attack on a bunker security system.

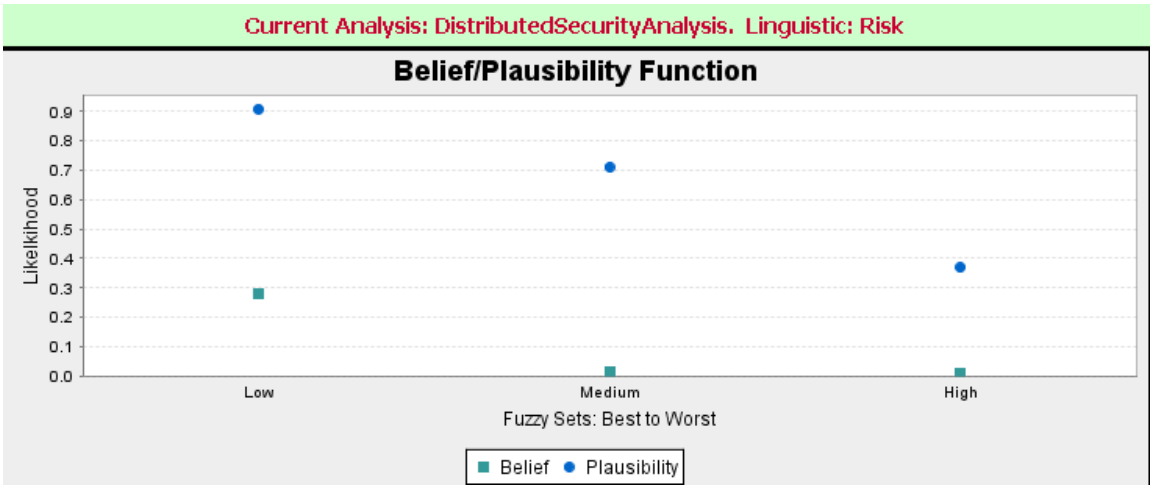

Figure 5b. Risk of an adversary attack on a distributed security system.

Conclusion

Future Development. The development of a workable and functional "distributed" security system is non-trivial, but the time may be fast approaching when the burden of maintaining a "bunker" based security may not be sustainable in the face of a determined, adaptable and technically capable adversary, especially as technology that can compromise "bunker" systems continues to improve at an accelerating pace.

Areas of research should include the development of systems engineering tools and techniques that would enable compartmentalized product development in order to minimize the amount of knowledge that can be exploited to compromise the overall security of the final product. Very closely aligned with design and development of the product and security is the logistics of the product lifecycle to ensure a robust product function with minimal potential for disruption and attack.

Another necessary area of research is the field of information, specifically, how should the information in a distributed security system be handled, encrypted, generated, stored, transmitted and employed to ensure both the proper function of the product and the security? With advances being made in knowledge management the question naturally arises as to whether a security system could be designed that does not depend on human supplied knowledge. In other words, the system itself would be "self securing" by relying on information that is autonomously generated and "known" only to the elements of the system, thus eliminating the human insider as a significant path for compromising security.

Besides the information within the system, there is also significant opportunity to acquire, process, and utilize information regarding the intent, capabilities and timeline of the adversary. The intelligence community is already gathering in vast amount of data, but reducing that to manageable information and actionable knowledge is a daunting task. Agent based computational systems can potentially offer "expert" assessment and options for both slowly developing security situations as well as help responders deal with the dynamic environments of force-on-force security events.

Closing Comment. This paper barely scratches the surface of the principles involved in "distributed" security and the application of these principles to real systems. While seemingly counterintuitive to conventional security concepts, systems that are based on a "distributed" security scheme could lower the asymmetry of today's threat environment, which could lower the risk, and cost of providing security. Much fruitful work can be done by Systems Engineering to develop and validate these principles and their application to diverse systems in this changing world.

References

Garcia, M. L., The Design and Evaluation of Physical Protection Systems, Butterworth Heinemann, Boston, 2001

De Spain, M., Griego, R., Verma, D., Addressing a Public Institution's Response to "Disruptive Technologies," CSER 2007, Stevens Institute of Technology, Hoboken, 2007

Darby, J., LinguisticBelief: A Java Application for Linguistic Evaluation Using Belief, Fuzzy Sets, and Approximate Reasoning, SAND2007-1299, Sandia National Laboratories, 2007

Biography

Mark J. De Spain has been an engineer at Sandia National Laboratories for over twenty years. He has worked in weapons components including sensing devices, firing sets and use control. Currently he is working as a use control systems engineer. He has a BSME from Oregon State University and an MSEE from the University of Portland.

Dr. John L. Darby earned a PhD in Nuclear Engineering from the University of Wisconsin. He is a registered professional engineer (nuclear) and is a Sun Certified Java programmer. He is the former Manager of Nuclear Engineering at the Davis Besse Nuclear Power plant, and former Chair of the Los Alamos National Laboratory Reactor Safety Committee. For 14 years he participated in the preparation and grading of the national professional engineering examination for nuclear engineers. He is currently a member of the technical staff at Sandia National Laboratories, Albuquerque. For the last five years, he has focused on developing and applying non-probabilistic techniques and software tools for the evaluation of risk, primarily to evaluate acts of terrorism where there is significant epistemic uncertainty.

Dr. Robert Cloutier is a Research Associate Professor in the School of Systems and Enterprises at Stevens Institute of Technology. He has over 20 years experience in systems engineering & architecting, software engineering, and project management in both commercial and defense industries. His research interests include model based systems engineering and systems architecting using UML/SysML, reference architectures, systems engineering patterns, and architecture management. His most resent publications include INCOSE Systems Engineering Journal, Enterprise Architect Journal, Telelogic North American Users Conference, and Conference for Systems Engineering Research.

Rob spent twelve years working for Boeing in Philadelphia primarily as a lead avionics engineer and an enterprise architect. During his seven years at Lockheed Martin he was a lead software engineer and a system architect on a number of efforts and proposals. As the lead software engineer and lead process engineer, he was part of the leadership team that worked with the Navy to move the Aegis combat system to an object oriented software product, using an iterative development process.

Joining Stevens faculty in 2007, Rob has taught courses and delivered workshops in systems engineering, system architecture for industry and government systems engineers; and architecture thinking for architecture thought leaders at Nokia. Rob has experience delivering coursework both in the classroom and online, and has developed courses for both venues. He also teaches MIS and Graduate courses for Eastern University in St. Davids, PA.

Rob belongs to the International Council on Systems Engineering (INCOSE), and is a member of the Technical Leadership Team and also belongs to IEEE and ACM. Rob received his Ph.D. in Systems Engineering from Stevens Institute of Technology, and also holds an M.B.A. from Eastern University, and a B.S. in Physical Science from the United States Naval Academy. He is an Adjunct Professor for Eastern University and chairs the Rowan University Electrical and Computer Engineering Department Industry Advisory Board. Finally, he and his wife raise puppies for The Seeing Eye to serve as guide dogs to the blind.