Research Paper

Creative Adversarial Vulnerability Assessments*

Edward G Bitzer III and Roger Johnston
Vulnerability Assessment Team
Los Alamos National Laboratory

*Editor's Note: This paper has not been peer reviewed.

> *If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.* *-- Sun Tzu*

During a press conference in May of 2002, then National Security Advisor Dr. Condoleezza Rice discussed the failure of the government to predict attacks similar o those that occurred on September 11, 2001. She stated that "I don't think anybody could have predicted that these people would take an airplane and slam it into the World Trade Center, take another one and slam it into the Pentagon; that they would try to use an airplane as a missile…"[1] Of course, that is exactly what happened. However, this paper is not meant as an indictment of the statements or ability of Dr. Rice, we use this example only because it is indicative of a greater problem among the United States intelligence/security communities and, we believe, the private security community as well. That problem, stated simply, is a lack of imagination. Indeed, the 9/11 Commission has also lamented such shortcomings. In their final report, the Commission succinctly states, "Imagination is not a gift usually associated with bureaucracies…It is therefore crucial to find ways of routinizing, even bureaucratizing, the exercise of imagination." To that end, we wish to share tools

[1] According to her testimony to the 9/11 Commission Dr. Rice commented about this statement. In her testimony Dr. Rice acknowledged that she had implied that no one could have imagined the threat of terrorists using planes as missiles. However, also in her testimony, Dr. Rice backed away from such statements saying "As I said to you in the private session, I probably should have said, 'I could not have imagined...'" such attacks. Retreating from such a statement was of course necessary because within days of Rice's initial comments at the May 2002 press conference, reports began to emerge that that someone *had* imagined such attacks. In fact, many such someone's had imagined such attacks including the intelligence community (in response to information about Libyans with similar plans for attacks on the WTC), Philippine authorities (who were told of plans for such attacks on CIA headquarters), a Justice Department lawyer, NORAD, Eric Harris and Dylan Klebold (the perpetrators of the Columbine High School massacre, and perhaps any number of Navy veterans who had experienced very real attacks of the same nature at the hands of Japanese Kamikaze pilots.

and techniques that may be helpful in brining the power of imagination to bear on the problems associated with security.

The authors of this paper are members of the Vulnerability Assessment Team (VAT) at Los Alamos National Laboratory. One major function of the VAT is to, as the name implies, conduct vulnerability assessments (or red teaming) in an attempt to discover weaknesses in physical security policies and procedures. In the course of these assessments, we strive to examine security not from the viewpoint of security professionals, but rather to put ourselves in the position of our adversaries. To think like the bad guys. And it is through this process (what is called *adversarial* vulnerability assessment), that we believe some of the most effective vulnerability assessments can be conducted. A full description of the 13 steps of the adversarial vulnerability assessment (AVA) process can be seen in an article written by Johnston (2004), and a full recitation of this process is beyond the scope of this paper. Instead, we will focus primarily on Step Four in that process. Johnston has identified this step, Brainstorming, as perhaps the most crucial step in conducting a successful vulnerability assessment. When this step is done well, an AVA can be a powerful tool for revealing major unforeseen vulnerabilities. When done poorly, AVA's are rendered no more useful than more traditional security walkthroughs.

Although this step has been called Brainstorming, the name can be somewhat misleading. In fact, the process can be viewed more broadly. Brainstorming is a particular technique (likely familiar to many) that can be very useful, but it is only one of a series of techniques that can be employed to come to the same ends: thinking imaginatively, or creatively, about potential vulnerabilities that might be present. It is a discussion of a series of these techniques that we will now turn.

Techniques for Thinking Creatively

Although it is somewhat novel in the security world psychologists, marketers and others have long been interested in ways to help teams of individuals to develop "outside-the-box" thinking. Through the course of this interest, a number of different ideas have developed. One of the first is the concept of brainstorming mentioned earlier. Others are variations, or evolutions, of the brainstorming concept. We hope to outline examples from each of these areas, as well as propose techniques not traditional thought of as creativity techniques, but which – when approached with the same sort of open-mindedness – can lead to similar results. As with the work of creativity theorists, we will start with brainstorming.

Brainstorming – There are a number of different writers and consultants who have promoted brainstorming as the answer to inducing creativity from a team. And it may be that there are as many processes of brainstorming as there are proponents. We are not especially convinced that any one process will be any more successful than any other. The bottom line is that most of these processes contain many of the same basic underlying traits. And it is our belief that as long as these traits are present, any process of brainstorming can be successful. Therefore, it is vital that any team leader, in this case VA team leaders, know what the underlying traits are, and apply those traits in a way that makes sense for their particular team. As such, we will outline the four basic traits for brainstorming so vulnerability assessors can use them in appropriate ways.

1) Establish an objective – Objectives are important for any number of activities, and brainstorming is no exception. The purpose of establishing objectives is to set a clear expectation of what the brainstorming session is intended to accomplish. The purpose of brainstorming is to allow the brain to run wild with ideas, but the ideas still must be directed to a particular cause. Objectives establish that cause and keep everyone on the same page. Remember, we are talking about an adversarial vulnerability assessment. As such, the right type of objectives would be something like, “The goal is to attack X facility” or “We are attempting to create havoc in Z community.” We know that this may feel very alien and uncomfortable for individuals who have spent their lives and careers attempting to prevent such attacks, but the objective must focus on compromising a particular building, security device, etc. It is our goal to “know” our enemy, as in the quote above from Sun Tzu. It may also be helpful to establish a time limit for the session. This helps the team members, and the team leader, keep the team on track and moving forward toward successfully completing an objective.

2) Lay out ground rules – There are a number of ground rules that should be put in place in order to allow for the most effective brainstorming. The first is to identify a recorder who will write down all ideas. The ideas should be written down in full view of everyone (such as a chalkboard, whiteboard, or flip charts). This serves two purposes including preventing, to the extent possible, the repeat of ideas and to allow individual members to work off of others’ ideas. Second, there should be no judging of any of the ideas that are generated, no matter how absurd they may appear. Many great ideas throughout history, including that the world is round or the personal computer, have at one time been viewed as crazy. The most effective way to stifle creative thinking is to judge ideas during the idea generation phase. Criticism and judgment will cause participants to be less likely to go out on a limb and bring up what may potentially be valuable ideas. Third, eliminate all distractions including cell phones, pagers and the possibility that anyone not in the brainstorming session could interrupt. Brainstorming works best when one idea can flow fluidly from another, distractions will make that impossible. All participants should shut off electronic communication equipment and it might be helpful to hold the

session somewhere away from traditional meeting areas. You want team members to think outside-the-box so get them outside the office.

3) Generate ideas – This is the meat of the brainstorming session. It is at this point that, as mentioned previously, there are a number of ways to go about this process. Perhaps a free-flow of ideas, with no order of who can speak and when, will work best. Perhaps all participants should be given a few minutes to share their ideas, with time afterwards for anyone to share additional ideas they have thought of as others were speaking. Maybe you will require that all participants give at least one idea, maybe no such requirement is made. The key, however, is that the team leader select the procedure which best fits the personalities of their team. Fit, however, does not always mean making everyone feel comfortable. You want the team to feel safe to share ideas, but the point is to get them to stretch to find interesting, viable, and novel ideas.

4) Select ideas – At this point, it is hoped, there will be a number of ideas that have been generated. Most likely, more ideas than can reasonably be dealt with. Therefore, a process of selecting which potential attacks to examine in more detail must take place. Criteria for selecting where to focus may be on the ease with which an attack could take place, the consequences if such an attack were to occur, some combination of these criteria, or other criteria altogether. It may be beneficial to allow group members to become proponents of one or a few ideas in order to more fully consider all alternatives (the group leader, especially a powerful or well respected leader, should refrain from this process as he or she may exert undue influence and cause groupthink to take hold). Finally, each group member should be given one or more votes to cast for the idea that they think deserves the most consideration. The ideas that receive the most votes should become the focus of the remainder of the AVA.

Nominal Group Technique – The nominal group technique (NGT) is an evolution on the traditional concept of brainstorming. The NGT technique was developed as a way to avoid some of the pitfalls of group work, such as social loafing and the desire for anonymity. Social loafing is the tendency for individuals within a group to exert less effort to a particular task than they would if they were working alone. Anonymity is of particular concern in the security field. For a variety of reasons, there is often a “shoot the messenger” response to those that surface concerns about security procedures and plans. NGT attempts to address these and other brainstorming issues by first requiring that team members conduct brainstorming sessions individually to develop as many ideas as they can. Then they submit their ideas, sometimes anonymously, to a central recorder who writes down everyone's ideas. It is only then that the whole group gets together to consider and evaluate each idea. Then the group as a whole will choose to accept ideas (or perhaps a combination of ideas) for the AVA. This selection process is often conducted in much the same way as the selection process in a brainstorming session.

SWOT Analysis – The process of conducting a SWOT analysis is probably very familiar to individuals with any management or strategic planning experience. A SWOT analysis gets its name from the four individual components that go into the analysis process. These four components are: strengths, weaknesses, opportunities, and threats. The basic idea behind a SWOT analysis is to identify areas that would fit under each of these four components, and then put each of these components together to find productive avenues for action. Although SWOT analysis is a fairly traditional strategic analysis technique, using it as part of an AVA is very untraditional. So we will describe in more detail how to conduct a SWOT analysis from an adversary's perspective.

1) Strengths – The first step in conducting an SWOT analysis is to identify the areas that are particular strengths to an organization (in this case the strengths of the adversary). Strengths are identified as internal to the organization. Examples of such strengths would include technical competence, an unblemished criminal background, or the ability to physically blend in with a crowd or their surroundings.

2) Weaknesses – The second part of the SWOT analysis is to identify weakness areas that the adversary might experience. Like strengths, weaknesses are internal areas within the organization. Examples of such weaknesses might include a tainted criminal background, the lack of appropriate access control metrics (e.g. keys, cards, passwords, or biometrics), or poor funding.

3) Opportunities – Third, one must identify the particular opportunities that exist for the adversary. Unlike strengths and weaknesses, opportunities are those areas that are external to the adversary, but in their operating environment. Examples of such opportunities might include knowledge of a particular timeline or planned route for the transfer of a valued commodity, knowledge of a particular type of access control system or guard schedule being used the target organization (your organization), or even a knowledgeable individual inside the target organization who could be bribed or coerced into giving valuable information.

4) Threats – The final step in the identification phase of the SWOT analysis is the identification of threats that the adversary might face. Like the opportunities, these would be in the adversary's

operating environment. Examples of threats might include such things as a well-trained and well-armed guard force at the target organization, police or intelligence services actively pursuing them, or an insider sympathetic to the adversary's target who may reveal their plans.

The second phase in the SWOT analysis is to combine the S's and W's with the O's and T's into a matrix. This process will create four strategy areas that can help in identifying the most valuable avenues for identifying potential adversarial action. The four strategy areas created include S-O strategies, S-T strategies, W-O strategies, and W-T strategies and would be presented in a form similar to the matrix below.

	Strengths	Weaknesses
Opportunities	S-O strategies	W-O strategies
Threats	S-T strategies	W-T strategies

S-O strategies outline particular areas that the adversary may be interested in exploiting. For example, high technical competence plus knowledge of particular access control systems might afford the adversary an opportunity to defeat such systems. S-T strategies indicate ways in which an adversary may use some of its strengths to help alleviate the potential impact of external threats. For example, using the ability to blend into their surroundings as a way to prevent confrontation with a well-armed guard force. W-O strategies provide the adversary guidance on ways to develop their internal organization to exploit a potential opportunity. An example would be gathering funds (which currently don't exist) in order to pay a knowledgeable insider for valuable information. Finally, W-T strategies identify the particular areas where an adversary would develop defensive plans for preventing the two areas from coming together. An example would be only recruiting or using operatives with clean criminal backgrounds, those who would not draw the attention of police or intelligence agencies.

After developing the particular strategy areas, from the perspective of the adversary, VA teams can develop counter-measures of their own to exploit actions that might be taken by an adversary. One possible example would be varying access control systems or layering systems on top of each other to prevent or deter adversaries from using those areas in an attack.

Conclusion

We believe that through use of the techniques described above, as well as any other technique that allow vulnerability assessors to think creatively, or imaginatively as the 9/11 Commission might call it, it is possible to conduct vulnerability assessments that are powerful tools in discovering and alleviating potential vulnerabilities that might exist. And although AVA is not the only tool that can be used to attempt to strengthen security, when used in combination with more traditional techniques such as security surveys and risk management practices, a more secure environment can be created.