AFRL-RI-RS-TR-2010-129

CENTER FOR INFRASTRUCTURE ASSURANCE AND SECURITY – ATTACK AND DEFEND EXERCISES

University of Texas at San Antonio

June 2010

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

AFRL-RI-RS-TR-2010-129 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/s/
WILLIAM J. MAXEY
Work Unit Manager

/s/
WARREN H. DEBANY, Jr.
Technical Advisor, Information Grid Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
JUNE 2010	Final	May 2002 – December 2009

4. TITLE AND SUBTITLE

CENTER FOR INFRASTRUCTURE ASSURANCE AND SECURITY – ATTACK AND DEFEND EXERCISES

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
F30602-02-1-0001

5c. PROGRAM ELEMENT NUMBER
33140F

6. AUTHOR(S)

Gregory B. White

5d. PROJECT NUMBER
CIAS

5e. TASK NUMBER
96

5f. WORK UNIT NUMBER
10

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
University of Texas at San Antonio
One UTSA Circle
San Antonio, TX 78249-1130

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/RIGA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TR-2010-129

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This effort developed the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA). It began in 2002 and was designed to build a center focusing on cyber security/information assurance issues at UTSA. The effort involved a number of cyber security/information assurance research projects. This encouraged faculty members to begin successful research activities in the area of cyber security. This was successful and a number of projects were begun which in turn helped to attract other researchers. One of the significant research activities was the development of a community cyber security exercise and the more technical attack/defend exercise concept. This led to a project which began to focus on the continued sustainment of the center and its focus on exercises. This eventually led to the development of the Community Cyber Security Maturity Model (CCSMM) which provides a structure for communities to use in evaluating their current cyber security posture as well as a roadmap to follow for them to improve their posture.

15. SUBJECT TERMS

Information Assurance; Cyber Security; Botnet; Steganography; Biometrics; Information Infrastructure

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			William J. Maxey
U	U	U	UU	29	19b. TELEPHONE NUMBER (*Include area code*) N/A

ABSTRACT

This report describes the activities that were conducted as part of the ongoing effort developing the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA). The project has gone through three development periods. The first, starting with the origination of the project, began in 2002 and was simply designed to help build a center focusing on cyber security/information assurance issues at UTSA. The second period began the next year when additional money was obtained which helped continue the development of the center and also helped by providing start-up funding for a number of cyber security/information assurance research projects. This money was used to help encourage existing faculty members to begin research activities in the area of cyber security. This was successful and a number of projects were begun which in turn helped to attract other researchers to the university – thus enhancing the center and the university itself. One of the significant research activities begun during this time was the development of the concept of a community cyber security exercise and the more technical attack/defend exercise concept. This led to the third period of funding for this project which began with the eventual elimination of the research "seed" money and focused on the continued sustainment of the center and its focus on exercises. Funding from this project along with funding from the Department of Homeland Security eventually led to the development of the Community Cyber Security Maturity Model (CCSMM) which provides a structure for communities to use in evaluating their current cyber security posture as well as a roadmap to follow for them to improve their posture. While it may at first seem like a subject more applicable to the Department of Homeland Security, the issues raised are important to the Department of Defense (DoD) as well because of the dependence of DoD facilities on the communities in which they reside. Thus, the project emphasized communities in which there was a significant DoD presence, especially those that hosted a major command. A number of exercises were conducted as part of this program and programs to help communities secure their infrastructures were successfully developed as part of the model. Ultimately, the program resulting from the funding received has to be viewed as a success since a strong cyber security center has been established at UTSA, a number of faculty members are involved in continued cyber security research efforts, and a model to help the nation's communities secure their cyber infrastructures has been created and is being implemented in several communities.

TABLE OF CONTENTS

SUMMARY

This report describes the activities that were part of a seven year effort supporting the creation of the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA) and the development of various research activities and programs as part of it. The funding provided incentives for a number of UTSA faculty to begin research programs in cyber security and information assurance areas. This has proven very successful and there are a strong cadre of faculty members now conducting research in these important areas in three different colleges at UTSA – Engineering, Science, and Business. Efforts in the program have also helped lead to the development of the Community Cyber Security Maturity Model (CCSMM) and the National Collegiate Cyber Defense Competition (NCCDC). A number of communities have now participated in cyber security exercises and awareness training as part of this effort and are arguably better prepared to deal with a cyber security incident affecting the community. With military installations relying so heavily on the infrastructures of the communities in which they reside, the argument could then be extended to state that the military installations are better off in those communities in which a cyber security exercise has been conducted. While much has been accomplished, there are numerous communities that have not conducted a cyber exercise and the ones that have are only just embarking on the development of a viable and sustainable cyber security program. The CCSMM has five levels and no community has progressed past the second level yet. As such, the communities are more aware of the issues and that they need to do something and are thus more prepared, but they have not accomplished everything they can do in order to be able to prevent cyber security attacks from severely impacting their infrastructures. A lot of work still needs to be accomplished.

1. INTRODUCTION

The Center for Infrastructure Assurance and Security (CIAS) was created at The University of Texas at San Antonio (UTSA) in the summer of 2001. The center received its first grant in early 2002 through a Congressional add to the Department of Defense (DoD) Appropriations Bill. This first amount was $2.5 million and was to be used to establish a security center at UTSA with no specific program or research specified. At the time no funding mechanism to get the money to UTSA was specified but a relationship was being worked with the Air Force's Air Intelligence Agency (AIA) in San Antonio. A method to provide the funding to UTSA was worked out which resulted in a relationship being established between the Air Force Research Laboratory (AFRL) and UTSA. The money then flowed from AIA, to AFRL and finally to UTSA. The CIAS hired its first two full-time employees in September, 2002 and started funding several security related research projects at the same time.

2. METHODS

Since the initial funding was not aimed at any specific topic but rather was to help the university establish a cyber security program, a method was required to reach out to existing faculty members to see who might be already engaged in cyber security research and who might be interested in developing their own cyber security research initiative. Initially, there was a handful of individuals who had already conducted some research in cyber security or information assurance but who did not have the funding to grow their individual programs. In order to help guide the establishment of projects that would be of interest to the Air Force, a call for proposals went out to UTSA faculty and the resulting submissions were evaluated by UTSA and Air Force personnel (from AIA) to identify the projects that might be of more interest to the Air Force. Since the goal was not to provide specific deliverables addressing previously identified problems the Air Force wanted to have solved, the a broad range of projects were selected with no specific deliverables beyond helping to establish their principle investigators as security researchers.

In addition to helping to jumpstart the research program at UTSA, establishment of the CIAS as a center at the university also helped with the overall establishment of the university's cyber security/information assurance program which led to the university obtaining the NSA (later DHS/NSA) designation as a Center of Academic Excellence in Information Assurance Education. Classes were developed and a major established at the university in Information Assurance at both the graduate and undergraduate levels. Later, concentrations in computer security were also added. DoD personnel immediately benefited from these programs as numerous military and DoD personnel began taking classes at the university leading to degrees in these needed areas.

3. RESULTS

The program was very successful in establishing not only the CIAS as a center of cyber security expertise, but also helping to encourage faculty members at the university to explore cyber security as a possible research area. In the first year of funding, four topics were initially selected as areas for investigation: steganography, cryptography, wireless security, and intrusion detection. These topics were chosen based on proposals submitted by UTSA faculty and inputs from local Air Force organizations. Subsequent years expanded on this initial set of topics and many more investigators were added to the program.

4. ESTABLISHED RESEARCH EFFORTS

What follows is a list and description of the various research projects that were funded under this effort. Many of the investigators for these projects continue to conduct research in these areas and new advances are being made though funding through this project stopped several years ago. As a result, the descriptions for the research projects come from reports provided at the conclusion of the research funding under this program.

4.1. Steganography Detection Tools

Steganography is the art of hiding information in a cover image so it is not readily apparent to a third party observer. There exist a variety of steganographic methods for embedding information in an image. Some of the more common methods are altering the LSB (least significant bit) of the pixels of the image, altering the palette of an RGB image, or altering parts of the image in the transform domain. Algorithms that embed information in the transform domain are usually more robust to common attacks and have less impact on the visual content of the cover image [3]. There are a variety of algorithms for hiding information in the transfer domain. The DCT, Fourier, or wavelet transforms are examples of the types of transforms that have been used.

This research effort was designed to explore possible methods to create a general steganographic detection tool that was not technique specific. Steganography has become an increasingly popular method on the Internet to hide information from both human and electronic monitoring. Although several tools have been developed by other researchers to detect steganographic files, they all are specific to a certain technique used to hide the information. Since new techniques are constantly being developed to hide information, current tools have proven to be inadequate. Researchers working on this project developed a global universal blind steganalysis method. Their method can localize the hidden information, it can capture stego information in small blocks, and it can work by using small training sets. Experimental comparisons of the performance of the new method showed better performance than commonly used schemes (was much faster and more accurate).

4.2. Intrusion Detection Systems

The Air Force has long been interested in several aspects of intrusion detection systems including long-term research into high-speed intrusion detection and (at the time of this research project) near-term examinations of current approaches to streamline data correlation and to reduce the amount of data an analyst must view (data reduction). Research included examination of the use of Field Programmable Gated Arrays to support intrusion detection in the multi-gigabit range and an effort designed to assist the Air Force Information Warfare Center (AFIWC) in re-designing the Air Force common intrusion database to enhance the daily operations of the Air Force Computer Emergency Response Team (AFCERT). The redesigned database would improve the speed of data searches and retrieval and would enable enhanced data mining techniques to examine intrusion data for "low and slow" attacks that were often not seen by then current operational techniques.

The project resulted in a new design of a data model to support statistical data mining with the then current Air Force intrusion detection system. It also created an architecture for the data layer of the project and software engineering methods to achieve the project goals. In addition, system performance with respect to IPv6 (which was then emerging as a potential problem for Air Force network systems) issues such as IPsec and enclaves was examined. On the hardware side, researchers were able to develop a scalable architecture for a high-speed IDS using FPGAs and then went on to implement it. The results were positive but were not viewed as a replacement for then planned advancements to the methods currently in use by the Air Force.

4.3. Cryptography

The goal of the project was to develop a basis for utilizing efficient encryption schemes in devices with low computing power and resources. It was believed that ECC Cryptography was appropriate for an efficient and secure encryption scheme. It is more efficient than the ubiquitous RSA based schemes because ECC utilizes smaller key sizes for comparable security.

Work on the development of API fronted software was accomplished. It was to help in integrating Elliptic Curve encryption/decryption at any layer in the network. Modest results in this regard were obtained though complete implementation was not accomplished before the end of the funding. The researcher continues to explore security topics so from the perspective of encouraging faculty members to conduct security research this project was successful.

4.4. Wireless Security Technology

Wireless technology is becoming increasingly popular and common in both voice and data networks. Because of its nature, however, wireless is potentially vulnerable to many different types of attacks. One aspect to examine was the problem of designing load balancing mechanisms with verification for heterogeneous distributed systems. The researcher implemented the state of the art Distributed Key Generation Protocol (DKG) in Open SSL (using secure sockets for network communication) then began working to obtain an Elliptic Curve based version of a DKG written in C++ and Secure Sockets. Further implementation included assumptions occurring in wireless technology.

A wireless research project explored the design of robust wireless networks that offer secure, continuous high-speed connectivity among the wireless nodes and to the available network infrastructure. Such networks consist of 100s to 1000s of wireless, mobile nodes spanning a wide area such as a metropolitan city. The design goal was to ensure the persistent wireless networks (PWNs) would be able to withstand terrorist attacks, which could cripple the hardware, and hacker attacks, which could contaminate and compromise the software. The project addressed network security at transport, routing, and MAC (medium access control) levels. The results of this project proved that noncolluding attacks by malicious nodes can be detected using an inexpensive crosscheck mechanism with pair-wise symmetric keys. Furthermore, it was also shown that the group of nodes that contain the attacking nodes can be identified. Previous methods only detected falsification of route information. The developed technique facilitated identification of such nodes as well.

4.5. Biometric Devices and Security

A study was conducted that was designed to examine various biometric techniques and determine their effectiveness. The attempt was made to pay particular attention to devices specifically in use by or which were planned to be used by the Air Force. The accuracy of biometric techniques was questionable at the time and it was not commonly known that they might not have provided the amount of increased assurance that vendors had promised. The report was completed and provided to the AIA liaison to UTSA.

4.6. Computer Forensic Course Development

A need existed for more computer forensic capable investigators both in the military and among civilian law enforcement agencies. This effort was designed to develop courses to train individuals in computer forensic techniques. Then current tools and techniques were examined for their adequacy and, as needed, new approaches were proposed. At the time, the number of individuals trained to find and preserve computer evidence had not increased at the same pace as that of the crimes being committed and the same situation still exists today. More investigators need to be trained and efficient techniques developed to locate and preserve evidence located on computer systems and networks. This effort resulted in the development and updating of computer forensics courses at the university.

4.7. Improving Bayesian Filtering for Spam Detection

The goal of this project was to improve Bayesian filtering algorithms for detecting spam email. The desire was to improve efficiency and effectiveness simultaneously. A comparison of the proposed algorithm (named SCOLA) versus other spam detection programs at the time (Bogofilter, CRM114, SpamAssassin, SpamBayes, and SpamProbe) was conducted. Bogofilter, SpamBayes, and SpamProbe used variants of Bayesian filtering. SpamAssassin used Bayesian filtering as part of its processing along with a fixed set of patterns that discriminated between spam and ham. CRM114 learned regular expressions. The comparison was performed on 3 email datasets. Overall, Bogofilter and SCOLA performed the best of these algorithms and were within 0.5% of each other on the three datasets. Bogofilter, however, had the advantage of learning incrementally while the version of SCOLA needed several passes over the emails.

4.8. Power-efficient mechanisms for detecting replay-based intruders in wireless ad hoc networks

This research effort was designed to detect replay-based intrusions that negatively impact routing protocols. It was hoped that initial research efforts and findings in this project would enable a better understanding of the problems in providing secure routing in ad hoc networks and lead to the development of a comprehensive plan to further investigate these problems. The researchers designed a MAC protocol to allow wireless nodes in MANETS to send their prioritized traffic in an efficient and guaranteed manner. A basic version in NS-2 was implemented. Based on the obtained results, the researchers reshaped the ideas and integrated new mechanisms to further improve the performance.

4.9. Privacy Preserving Database Operations

This research effort was designed to develop a privacy preserving similarity search, privacy preserving sequence comparison, privacy preserving indexing and schemes to control access to databases. A generic privacy preserving similarity search scheme for norm spaces was developed based on bloom filters that can be used to control access to databases. This scheme denies access to some users if these users are trying to learn contents of the proprietary databases. A bloom filter based compression scheme for bitmap indices was also developed. Researchers developed efficient methods to discover databases using computational geometry guided techniques. For datasets with 1000 elements, initial results required about 50,000 queries to discover the data. Using a different approach researchers were able to reduce the number of queries required to 20,000.

4.10. Hiding Information from Machines

This research effort is designed to explore ways to hide information from machines, in contrast to the usual goal of hiding information from humans. The prototype environment is a modern battlefield filled with autonomous robots, where one wishes to provide information to humans or to machines under real-time human control in a way that the autonomous robots will not recognize. The researcher explored techniques that were basically similar to so-called CAPTCHAs: software used to detect the presence of humans. The research did not yield any other innovative approaches and funding was dropped.

4.11. Countering Malicious and Fast Spreading Worms

The objective of this research effort was to deal with worms that are fast spreading and malicious. In order to slow down fast-spreading worms, the researcher was interested in answering questions such as: How should anomaly detection sensors (e.g., Honeypots, Network Telescopes) be deployed so that their power is maximized? How can we make sure anomaly detection sensors will not be avoided or bypassed by worms? How can we proactively generate worm signatures? How can we mathematically model worms more realistically? The researcher was able to develop a scheme to automatically detect malicious imposter emails. Another technique was developed to automatically detect malicious code incurred request.

4.12. Learning Semantic Content for Image Indexing

This objective of this project was to examine the problem of finding a desired image in a large collection given the limitations of traditional text-based indexing at that time. Approaches at that time led to an upsurge in content-based image retrieval (CBIR) but CBIR had its own limitations. The techniques current at that time were restricted to matching image appearance using primitive features such as color, texture, and shape. Researchers addressed the problem in several phases and a novel hybrid dimension reduction technique for classification based on the hybrid analysis of principal component analysis (PCA) and linear discriminant analysis (LDA) was developed as well as a technique to conduct self-supervised learning based on discriminative nonlinear features for semantic image indexing. Tests on the developed approaches showed that the approaches were effective in accomplishing their goals.

4.13. Bimodal Biometrics: Fusion of Finger Print and Voice Print for Enhanced Biometric Authentication

This research effort was designed to investigate the fusion of two widely used bio-prints, specifically fingerprints and voiceprints. The researchers wanted to develop algorithms that would increase the accuracy and reduce the processing time of recognition. They also wanted to investigate the relative merits and demerits of fusion at different levels. The researchers ended up testing an off-the-shelf system for verifying identity at a simulated border crossing. The system was based on a configuration that included delivering a fingerprint scanning device to individuals in a car that was waiting in a queue. The finger fitting scanner was connected to a light laptop computer that, in-turn was connected to a wireless transmitter/receiver that used Bluetooth technology. A server was simulated to be in a kiosk or office, behind a door or wall. This system, in turn was connected, using its USB port to a cable that could be up to ten meters in length and connected to another wireless transmitter/receiver that used Bluetooth technology. The system, including off-the-shelf software proved that researchers could deploy such a system completely with off-the-shelf components. Addition of voice recognition was to follow.

5. EARLY EXERCISE EFFORTS

A separate effort, initially listed among the other research topics, was the development of what was referred to originally as "attack and defend" exercises. This work was as a result of cyber security exercises developed and conducted by the CIAS. The exercise effort was started in March, 2002 when a challenge was issued by Congressman Ciro Rodriguez to the City of San Antonio, UTSA, Bexar County, and AIA. The challenge was to conduct a community cyber security exercise to evaluate whether the community was prepared to prevent, detect, and respond to a potential cyber attack from a terrorist organization. UTSA took the lead in the effort with significant guidance from personnel in the Air Force. The Air Force was involved for two reasons. The first was the expertise that was resident at AIA in cyber security (then the home of the Air Force Information Warfare Center and the Air Force Computer Emergency Response Team). The question to be answered was how any of this expertise might be used to help the community in case of such an attack. The other reason for their involvement was to see how dependant the military installation was on local infrastructures and for the Air Force to learn how an attack on the community might affect their ability to conduct operations and accomplish their own missions. The exercise was called Dark Screen and it quickly showed both how unprepared the community was for such an attack and how little the military installations understood about their dependence on local infrastructures. As a result of these significant lessons learned, community exercises were added to the list of research topics that the CIAS pursued as part of the money they received from this project.

The goal for the attack and defend exercise effort is to develop a program that can be used to help prepare communities (and later states) to prevent, detect, respond to, and recover from a cyber security attack on the community (or state). As was mentioned, this is important to the DoD because of the tremendous dependence on community infrastructures in areas in which there is a significant DoD presence. It is important for the community to be prepared so that attacks will not incapacitate the community and affect the ability of the DoD installation to conduct operations and fulfill its mission. The DoD installations need to understand their dependence and understand how they are affected by the community infrastructures and how they would react in the event of an attack on the community. Both entities need to have in place agreements addressing how they will interact in the event of a cyber incident affecting them and how they can help each other.

6. EVOLVING PROGRAM

After the initial success of the Dark Screen exercise in San Antonio, there was interest in having the CIAS conduct exercises in other communities as well. The CIAS also became involved in conducting a number of sector-based cyber exercises (e.g. financial services, oil and gas, chemical, IT) which were funded not through this project but through funding from the U.S. Secret Service and their electronic crimes task forces. The experience gained from conducting these exercises, a second community exercise in San Antonio and another exercise in Corpus Christi, Texas, convinced the CIAS of the importance of these activities in helping organizations and communities become aware of the implications of a cyber attack on their infrastructures. Consequently, a number of exercises were scheduled in communities in which there was a "significant DoD presence".

The Corpus Christi exercise was conducted a few months after the second exercise was completed in San Antonio. The goal was to see if the lessons learned in conducting a community cyber security exercise in San Antonio were transferable to other communities. Just like the exercises in San Antonio, the exercise in Corpus Christ was a tremendous success in terms of making community members more aware of the potential effects that a cyber security event could have on their community. With the success of these two exercises, the desire was to take the program to other communities as well. Del Rio, TX followed in May, 2005 then Dayton, OH later that same year. The next year Hampton Roads (Virginia Beach) was added followed by Great Falls, MT and Honolulu, HI the following. The goal had been to engage communities in which there was a significant DoD presence – specifically those in which a major command was located or that constituted a significant part of the community. Other communities were approached (Colorado Springs, Omaha, and Tampa) in order to try and arrange an exercise in those communities as well but there was not enough interest by the local community leaders to ensure that the program would accomplish its goals. Despite a significant amount of time being spent with local and state leaders for these communities, the efforts were eventually tabled because it became apparent that they were not ready to consider cyber security at the time.

A significant development occurred during 2007. While the initial results from the communities was very positive in that the CIAS had been successful in helping community and local DoD officials aware of the cyber threat and possibility for a cyber incident to impact the community/DoD installation, the question as to whether any long-term change had actually occurred was raised. The CIAS took a look at the communities in which exercises had been conducted and was disappointed to learn that while the community leaders had been made aware of the potential impact of a cyber security event, they were struggling with what they needed to do in the community. They were aware it was a problem, they just didn't know what they needed to do in order to address the issue. As a result of this discovery, the exercises in 2007 were modified to add additional training before and after the exercises and the creation of a new model for community cyber security began.

Initial efforts in the communities had been centered on helping communities learn how to conduct a community (and later state) cyber security exercise. The belief at first was that by conducting an exercise the community could be made aware of the issues and would then be prepared to develop a cyber security program to secure the various cyber infrastructures within the community. What became apparent after conducting several exercises and later taking a look at what the communities had implemented was that more than an exercise was needed. The exercise served as a tremendous tool to make individuals aware of the issues. After each exercise, community leaders better understood how they could be affected by a cyber attack and the local military installations better understood their dependence on the community. What was not the case, however, was that this was sufficient for the community to then on its own begin the process of developing their own security program. This led to the research and development of the Community Cyber Security Maturity Model (CCSMM) which can serve as a yardstick for measuring how prepared a community is for a cyber attack and also as a roadmap for the steps a community needs to take to further develop their capabilities. The goal is to help communities to establish a viable and sustainable cyber security program. Beginning with the exercises in 2007, all subsequent community exercises attempted to use this model to help the communities develop their own viable and sustainable cyber security programs.

7. THE CCSMM

The Community Cyber Security Maturity Model outlines five levels of preparedness and identifies other activities such as training, incident response, and further exercises that are needed for communities to advance their cyber security posture. Funding from this project has helped with research and development of these other activities and the model itself. Additional funding from the Department of Homeland Security (DHS) has aided by allowing for the development of cyber security training courses that can be used as part of the program implementing the model. Funding from DHS has also helped pay for cyber security exercises in communities (see the list in Appendix B for a list of all exercises that have been conducted by the CIAS).

Each of the maturity levels in the model have been assigned a name indicative of the types of threats and activities being addressed at the level. The first level is labeled "Initial" which implies that this is where all communities will start as they embark on developing their cyber security program. Community leaders at this level have minimum awareness of the cyber security problem, there is little to no sharing of information about cyber security issues within the community, there are few if any cyber security policies and procedures and cyber has not been incorporated into the community's continuity of operations plan. The second level is labeled "Advanced" which implies that the community has finally advanced to a point where community leaders are aware that cyber security is an issue and that they should be concerned about it, informal information sharing about cyber security issues is taking place, initial policies and procedures have been developed, and cyber security exercises (at least tabletop exercises) are being conducted. The term "advanced" is somewhat political in that community leaders do not want to have their community labeled as only being "partly" secure. "Advanced" allows them to tell their constituents that the community is doing something to address this problem. While the title is "advanced", there is still much for the community to do in order for it to have a viable and sustainable program capable of addressing all cyber security threats. Level 3 of the model is "Self Assessed" which implies that the community is able to conduct a number of security related activities on its own. This is the first real level where the community can say that it has a "sustainable" security program. Up to this point, community programs will need a tremendous amount of external pressure in order for them to keep going. The natural tendency will be to let cyber security initiatives die as other disasters or priorities are faced by the community. At this level the community has introduced a formal program for sharing of cyber security information and community leaders are promoting cyber security awareness. At this level communities also will have cyber security incorporated into their normal exercise program and will have considered cyber in the continuity of operations program. Level 4 of the model is "Integrated". This level introduces a new concept – the idea that the security of the community relies not just on the community itself but on external entities as well. The state and other communities can have an impact on the ability for a community to effectively address cyber

security events – especially in the early stages where indications may lead to warnings of a pending attack before it begins. At this level the individual citizens are also engaged in securing their own assets and much like community watch programs can help with a community's physical security, the actions of individual citizens in securing their own assets and helping to secure the cyber assets they use at their place of employment can enhance the protection of the community against a cyber attack. elements are designed to develop better and more proactive methods to detect and respond to attacks. Level 5, "Vanguard", implies that the community is concerned with more than just its own security posture but is actually helping other communities and local businesses see cyber security as a business imperative. The characteristics of communities at the different levels is shown in the following diagram.

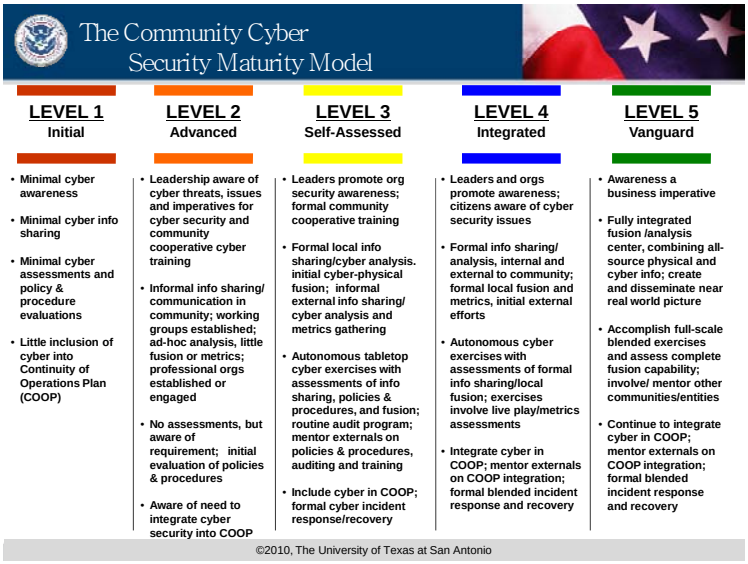

Figure 1: Community Cyber Security Maturity Model (CCSMM) 5 Levels

After the development of the initial two-dimensional model of the CCSMM as shown above, it soon became obvious that at the upper levels of the model more was involved. As stated in the brief description of the Level 4 characteristics, communities at this level are sharing information with the state and with other communities as well. It soon became obvious that the model really isn't a two-dimensional model, but is a three-dimensional model. In order for the community to be conducting information sharing activities with the state implies that the state has an information sharing program of its own – but where did that come from and how did that start? If there is a maturity model and process for a community, it follows that a state should also have a similar process and model as well. Looking in the other direction, for a community to be secure at the upper levels of the model means that individual organizations within the community need to also be secured to some level or the organization could become the weak link from which an attack on the community could be launched. This is especially true for organizations within the community that are part of the various critical infrastructures (e.g. banking and finance, energy, water, emergency services, etc.). The model was therefore expanded into the three-dimensional model depicted below.

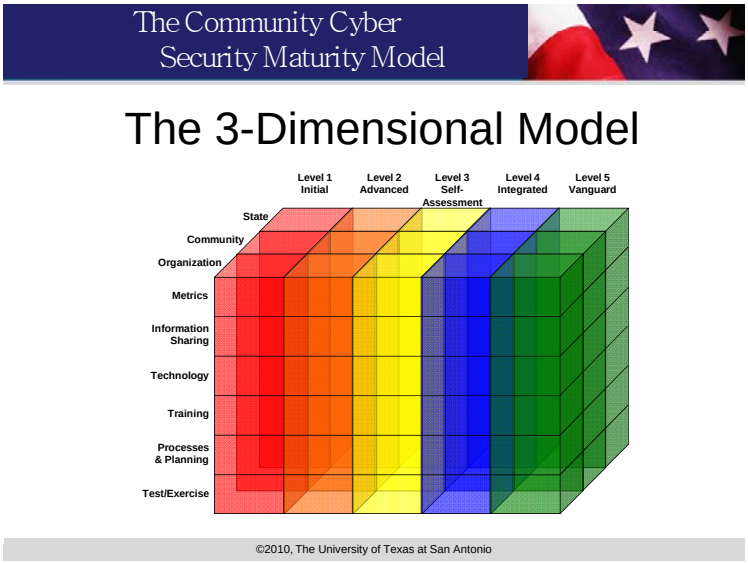

Figure 2: Community Cyber Security Maturity Model (CCSMM) 3 Dimensional Model

The 3-Dimensional model can actually be expanded beyond the organization, community, and state levels as well. It can easily be argued that another two rows should be added representing the nation on one end and individual citizens on the other. The model could even then be expanded to become an international model as well. In the above model various items are listed along the y-axis. These represent some of the activities/elements that can be found at the various levels of the model. Each individual block within the model can be examined to reveal the various pieces that make up that block. For example, the Level 1 community training block would include training courses designed to start individuals within the community on their path to cyber security awareness. The CIAS has spent time identifying various blocks of the model and finding low- and no-cost solutions for these blocks. The reason is simple – communities currently do not have large budgets to address cyber security. If anything is to happen at this point (the lower levels of the model), it will have to be at a very minimal cost. Fortunately there are a number of organizations that have developed training and awareness materials, tools, and guidelines for best practices that are freely available. Part of the program developed is to make communities aware of the opportunities to obtain these materials. It should be noted that while much work has been accomplished to "flesh out" the model and to complete the blocks, much still needs to be done on the model. This is especially true for the upper levels of the model where the characteristics are known that would identify a community as being at that level, but the training, technology, and guidelines required simply do not exist at this point. What is fairly well understood at this point, however, is what is needed in the lower levels of the model.

With the claim that more is needed to help a community establish a viable and sustainable cyber security program than just conducting an exercise, it is instructive to examine the program that has been established by the CIAS to accomplish this goal. The following steps represent the activities performed as the CIAS works with a community to help them establish their program:

1) An initial contact meeting with community leaders is set up. It is important to note that this is not with the IT director for the city, but rather somebody from the mayor's office. What is almost certainly true is that the IT staff in the community probably already understand much about the cyber security threat – it is the other community leaders that need to understand what the issues are. Without having all community leaders understand, there is little chance that a real program can be implemented.
2) Community leaders attend the "Leading Cyber Security" course which discusses the impact cyber security events can have on a community. This is designed for leaders and not IT personnel.
3) Planning conferences are held to plan for the first cyber security exercise which is designed to be an awareness tabletop exercise.
4) The first cyber security exercise is held. Again, the participants should NOT be IT personnel from across the community but rather community leaders and managers.

The object is to have these leaders understand what can happen if they lose the various cyber infrastructures within the community and by thus making them aware, having them help institute changes.

5) An after action report workshop is held. This workshop does more than simply present the findings of the exercise but instead is an opportunity for the facilitator to help the community identify who (or what organization) is responsible for implementing the various changes that are identified in the after action report.
6) A cyber security course is presented for IT personnel to help them learn more about what they need to do to help secure not just their own organizations but how the security of their organization can impact the security of the community.
7) Additional workshops are held in the community where security experts can help the various organizations develop their own policies and procedures and determine what technical solutions might be appropriate for various community organizations.
8) Planning begins for a second community tabletop exercise
9) The second exercise examines other elements needed to advance from Level 1 to Level 2 of the model. A major aspect of this exercise is information sharing between the various sectors and organizations within the community.
10) The after action report for the second exercise is delivered and a second workshop is held to help the community identify who/which organization will be responsible for implementing the lessons learned from the second exercise.

At this point, the community is well on its way to becoming a Level 2 community. The CIAS has attempted to work with more than one community in a given state where possible. This allows for the communities to talk with each other and to compare what they are doing. It also sets up a third exercise which is a state-level exercise in which the two communities conduct simultaneous exercises along with a state cell and the information sharing mechanisms that have been developed can be exercised. The program has been working well and the indications at the present time are that the communities implementing the model are better prepared to address cyber security events than were the earlier communities the CIAS worked with which only conducted the cyber security exercise.

8. RELATIONSHIP TO DHS

The DoD funding has been used to help prepare communities in areas in which there is a significant DoD presence. The CIAS realized, however, that the same issues applied to other communities around the nation as well. In 2004 funding was sought and obtained from the Department of Homeland Security (DHS) to develop a training program to teach communities how to conduct their own cyber security exercise. Later, when it was realized that more than just an exercise was required by the communities, an additional grant was applied for and received through the DHS to develop a series of training courses for states and communities on a variety of cyber security issues. The CIAS is one of four cyber training partners that DHS is now using to develop and deliver cyber security courses around the nation.

It is important to point out that both the DHS and DoD are benefiting from this program. When a community with a significant DoD presence was slated for an exercise, the CIAS first prepared community leaders for the exercise with a series of training briefings and courses that have been developed through DHS funding. Follow-on courses delivered after the exercise is conducted, also developed with DHS funding, are also presented to the communities. Much of what a community needs to do in order to advance, however, is still to be developed. The DoD needs secure communities to ensure their installations can operate. In essence, the DoD funding pushed the research and development of the CCSMM and the identification of its components such as the exercises and DHS funding has been obtained to take the lessons learned from these efforts and to “mainstream” them for use within any community within the nation. Exercises within DoD communities are tailored for their environment which includes ensuring representatives from local DoD installations participate and understand their roles within the community.

9. NCCDC

The Cyber Defense Exercise (CDX) is a program begun at the service academies to help prepare the "next generation of cyber warriors". It is a competition between the academies (with the Naval Postgraduate School and the Air Force Institute of Technology participating but not being eligible for the trophy) to determine which can best prepare their students to defend a network against a team of attackers (from NSA and other organizations). The competition has been conducted for a number of years and has been very successful at motivating students and encouraging them to consider a career in cyber security. A workshop held in 2004 in San Antonio (funded by the National Science Foundation) examine the value of doing the same thing at the collegiate level for all schools. After this workshop, the CIAS conducted the first open-category competition of this sort. Called the Collegiate Cyber Defense Competition, it was held in April 2005. Later that year plans were announced to conduct a national competition with regional qualifiers. The National Collegiate Cyber Defense Competition national championship was first conducted in 2006 and has been conducted annually since. This competition has been examined by DoD personnel and was also identified in the Policy Review out of the White House as a program that should be supported more fully. The first year of the national championship a team composed of members from the various service academies participated. Since then the CDX has occurred too closely to the NCCDC for the service academies to participate. The value of contests such as this has been recognized by the Air Force who has recently instituted a cyber security contest at the AFSPC Guardian Challenge event.

10.CONCLUSION

With the original purpose of the program to establish a center at UTSA, the project has been a tremendous success. Not only has a center been established (the CIAS), but a number of faculty members have started cyber security research programs influencing a number of students in a similar manner. The center has been heavily involved in a new arena – a cyber security exercise program. This started as a result of external factors, but has become a significant part of what the center accomplishes. In fact, the CIAS has now conducted more cyber security exercises than any other organization and has developed a program to help states and communities to establish viable and sustainable cyber security programs. The center is now defining processes and procedures for state and community activity that have not been defined before. The CIAS has become the de facto national leader in state and community programs. In addition, the center has established the National Collegiate Cyber Defense Competition which has proven extremely successful. Based on the original purpose of the funding for this program, it has been a tremendous success. The center has become nationally recognized and the university has established a strong cyber security research program.

LIST OF ACRONYMS

CIAS	Center for Infrastructure Assurance and Security
UTSA	University of Texas of San Antonio
CCSMM	Community Cyber Security Maturity Model
DoD	Department of Defense
NCCD	National Collegiate Cyber Defense Competition
AIA	Air Intelligence Agency
AFRL	Air Force Research Laboratory
LSB	Least Significant Bit
AFIWC	Air Force Information Warfare Center
AFCERT	Air Force Computer Emergency Response Team
DKG	Distributed Key Generation
PWNs	Persistent Wireless Networks
MAC	Medium Access Control
CBIR	Content-Based Image Retrieval
PCA	Principal Component Analysis
LDA	Linear Discriminate Analysis
DHS	Department of Homeland Security
CDX	Cyber Defense Exercise

APPENDIX
List of Exercises Completed

The following is a list of the cyber security exercises conducted by the CIAS. Not all have been paid for through this project, but all have contributed to the body of knowledge about sectors, states, and communities that has allowed the CIAS to develop the CCSMM.

San Antonio, Dark Screen Phase I (Lackland AFB)	13 September 2002
New York, NY (Financial Services Sector)	6 March 2003
San Antonio, Dark Screen Phase III (Lackland AFB)	15-24 September 2003
Chicago, IL (Financial Services Sector)	19,20 October 2003
San Francisco, CA (IT Sector)	5,6 November 2003
Corpus Christi, TX	4 February 2004
Houston, TX (Oil and Gas Sector)	18,19 February 2004
St Petersburg, FL (Financial Services Sector)	20,21 April 2004
Miami, FL (ISAC Congress)	14 October 2004
Baltimore, MD (Chemical Sector)	1,2 February 2005
Del Rio, TX (Laughlin AFB)	12 May 2005
Oklahoma City I (OK State Exercise)	1 December 2005
Dayton, OH (Wright-Patterson AFB)	12 December 2005
Hampton Roads, VA (Langley AFB)	28 February 2006
TX State Multi-Community (Plano, Tyler, Austin)	12 July 2006
Oklahoma City II (OK State Exercise)	7 December 2006
Great Falls, MT (Malmstrom AFB)	26 June 2007
Honolulu, HI (Hickam AFB)	17 July 2007
Tallahassee, FL (FL Dept of Law Enforcement)	9 October 2007
Tampa, FL (FL Dept of Law Enforcement)	12 October 2007
Ponte Vedra, FL (FL Dept of Law Enforcement)	19 October 2007
Ft. Lauderdale, FL (FL Dept of Law Enforcement)	23 October 2007
Bossier-City/Shreveport I, LA (Barksdale AFB)	15 July 2008
Rhode Island Cyber Terrorism Task Force	15 September 2008
El Paso, TX (Fort Bliss)	30 January 2009
Alexandria/Pineville, LA (Fort Polk)	7 May 2009
Dover I, DE (Dover AFB)	9 June 2009
Wilmington I, DE	25 June 2009
Tallahassee, FL (FDLE II)	15 October 2009
Lakeland, FL (FDLE II)	19 October 2009
West Palm Beach, FL (FDLE II)	22 October 2009
Sacramento, CA	5 November 2009
Palo Alto, CA	17 November 2009

Austin, TX	3 December 2009
Bossier City/Shreveport II, LA (Barksdale AFB)	8 December 2009
San Antonio, TX (Lackland AFB)	15 January 2010

In addition to the above exercises that the CIAS developed and delivered, the center has also participated in Cyberstorm I and II (the DHS national cyber security exercises) and will also participate in Cyber Storm III in Fall of 2010.