Using DoDAF As A Penetration Testing Tool

C.W. Perr, Christopher Harrison, Daniel Compton, J.A. Hamilton, Jr., Ph.D., *Auburn University*

Abstract - The penetration testing process, or the evaluation of a system for potential vulnerabilities, is a crucial factor in ensuring system security and stability. At its core, this process involves the art of analyzing and subsequently decomposing an inherently complex system into its constituent interoperable subsystems. It seems intuitive that, for the purposes of standardizing and expediting this process, one might employ the use of the very tools used in the construction of a target system in its decomposition. To that end, our team has chosen to use a sufficiently robust architectural modeling framework – the Department of Defense Architecture Format (DoDAF) – to aid in the decomposition of a sufficiently complex, black-box system in the context of the penetration testing process. The target system is the centrally managed student ID card system, which controls access to various services and facilities on campus.

Index terms – Software engineering, penetration testing, architecture, Department of Defense Architecture Framework, Open Source Security Testing Methodology Manual

I. INTRODUCTION

Hardware and software systems are the metaphorical heartbeat of contemporary industrial society. The integration of these hardware and software systems through modern communication vectors has elicited an unprecedented advance in humanity's ability to disseminate information. With this improved communication infrastructure and the subsequent proliferation of mobile devices, information technology is more accessible than ever. Therefore, the digital divide may soon be a thing of the past.

The driving force behind this rapid growth is the user's desire to be connected to sources of information at all times. From our seats on the bus we can now check our Facebook page, buy a plane ticket, and pay our credit card bill. As a result, the only economic sector in the United States anticipating substantial growth is the technology sector. This is due to the "New Era of Personal Computing"[1], an era driven by wireless mobile devices finding their way into the hands of more individuals, and those individuals using that technology to collectively push vast amounts of information across the web. Unfortunately, there is a serious downside to this increased information flow.

In a wirelessly connected population the surface area of vulnerabilities for the malicious attacker increases. Users demand usability in their devices, and the common trade off in device design is usability for security. Secure systems are viewed as unusable, and consumers ignore unusable systems. Due to consumer demands, developers spend an inordinate amount of time improving system usability rather than on the prevention of system misuse and the resolution of known vulnerabilities. This does not need to be the case.

System design can be adjusted to include a security mindset, which will aid in usability and provide a better view of the level of security and vulnerabilities found in a system. This can help us avoid a situation in our system that is known as the "Firesheep Effect.".

The "Firesheep Effect", which derives its name from a software tool written by Eric Butler, serves as a real world example of the lax attitude that many developers display towards system security. By utilizing a well-known vulnerability in the Transportation Layer, namely the lack of end-to-end encryption for HTTP data, Butler was able to make a tool that allowed malicious users to access to a target user's personal information. With its easy to use interface, Firesheep made this exploit accessible to Internet users who were otherwise devoid of security knowledge. This widespread availability, in turn, greatly expanded the impact of the security threat. Consequently, user data from major networking sites like "Facebook" and "Twitter", was compromised, and security fixes were finally implemented in order to mitigate the damage caused by the tool [2].

In order to rectify this issue we decided to integrate a modern penetration testing methodology with an evolving systems architecture toolset to create an educational architecture level document. This is used to inform decision makers on security level requirements, educate users on security procedures, and ensure compliance with basic design and standards across a complex system. In this way we create a 'picture' that non-technical decision makers can use to augment understanding of the security risks inherent in the pervasive use of technology.

II. THE IDEA

The idea for this project was originally conceived during a brainstorming session on ways to address security concerns early in the systems engineering process. It seemed obvious that a reactive approach to security was a

ISBN 1-933510-96-X/$15.00

poor strategy, and that such an approach would certainly lead to system abuse and consequently instability. Therefore, it was decided that a proactive approach, like penetration testing, should be included with the systems engineering process. In other words, systems engineering principles should be used to expand and augment current penetration testing methodologies. In turn, this modified methodology should be used to verify system security. If, while developing the penetration tests used to verify the security of a system, we were able to recreate the architecture of the system in a double-blind fashion then we could show that the actual product mirrored the standards and the design that were though of before production.

To take this further we selected an architecture tool that fulfilled our needs, the Department of Defense Architecture Framework version 2.02 (DoDAF), and then searched for a penetration testing methodology. DoDAF was chosen due to its provision of several key functionalities, which distinguish it from other architecture formats. Namely, DoDAF provides unique operational views, which deliver a robust solution to high-level modeling and the visualization of information flow. Moreover, because DoDAF is a Department of Defense standard, it already has a strong governmental presence, and many DoD employees are familiar with its use. DoDAF's design lends itself well to the intent of our work because non-technical individuals can easily interpret the resulting documents from DoDAF. Finally, DoDAF can be used use to focus on traceability of data, where it is travelling, and the security precautions taken to protect it.

The next selection was to choose our penetration testing methodology. Numerous valid options were available, and a good deal of research had to be done to choose the methodology that best suited our needs. The main methodologies under consideration were the Information Systems Security Assessment Framework (ISSAF), the Open Web Application Security Project (OWASP), and the Open Source Security Testing Methodology Manual (OSSTMM3).

Based on the available information, we chose OSSTMM3. The choice to go with OSSTMM3 was based on how well DoDAF and OSSTMM3 dovetailed together. We found all three methodologies to be sufficiently robust with regard to security analysis, but OSSTMM3 provided the clearest resulting documentation while its strict adherence to a scientific process resulted in the highest level of integration possible with DoDAF.

To demonstrate why OSSTMM3 was the apparent choice, it is vital to discuss in depth the advantages of OSSTMM3. OSSTMM3 defines a robust and clearly defined methodology for conducting penetration tests across a wide variety of systems. The methodology defined by OSSTMM3 consists of a semi-linear series of steps that outline the penetration testing process. One begins by defining system *assets,* or those system components that one wishes to protect from malicious attack. After recognizing system assets, one defines the *scope* of the penetration test, which consists of all subsystems and system components that interact with the assets. Areas found to be within scope are analyzed, and systems data derived from the analysis is then used to generate the penetration tests. In turn, these penetration tests allow analysts to identify and resolve real system vulnerabilities.

The sheer number of systems that OSSTMM3 can analyze demonstrates the raw flexibility inherent in its design. In summary, OSSTMM3 can be applied to any system which is comprised by *scope-able* subsystems, or systems which are comprised of Telecommunications and Data Networks (COMSEC), Physical and Human security channels (PHYSSEC), and the full spectrum of Wireless Security Channels (SPECSEC).

Because the successful application of the penetration testing process requires a strong knowledge of the target system for the generation of penetration tests, the system analysis phase is of central importance. Unfortunately, OSSTMM3's emphasis on the system analysis phase is lacking, and will not suffice. To resolve this issue, we must supplement the system analysis phase of OSSTMM3 with a sufficiently robust, external systems analysis tool. Hence, the necessary inclusion of DoDAF architecture.

DoDAF is an architecture model for organizing complex system designs into a series of complimentary viewpoints. The views in DoDAF are designed to model everything from the organizations involved to the processes taking place to the different levels of the solution system. The focus with DoDAF is on an iterative process with a variable scope that fully articulates a system at all levels. This is almost a perfect fit for the intent of OSSTMM3.

DoDAF will allow us to decompose the system at varying levels of abstraction, which fills in the DoDAF viewpoints with the information that is readily available or can be obtained from an outside penetration tester. These viewpoints can then be juxtaposed with the original DoDAF documentation to judge whether the system truly mirrors what was intended and if the standards are met. Adding compliance testing to go along with the penetration testing further enhances the usefulness of the procedure.

It is also important to explain why OSSTMM3 and DoDAF are necessary for this project. OSSTMM3 and DoDAF can, when combined, create a full spectrum of documents that clearly answer the main security questions in both graphically and report fashion. The final document represents the current state of the implemented

system, where the vulnerabilities are, and what defenses exist. The provided information gives insight into the level of the security, where it is located, and organizes the system information into an easily updated graphic explaining the system functions.

An additional feature to the generated documents is that they can be used to aid in incident response. The document quickly demarcates the sections of the system that were compromised, efficiently tells the investigator where the attacker was able to penetrate, and outlines what information was exposed.

III. The Target

For the purposes of our project we needed a target system. This had to be a system that we had access to, could readily view but did not have a penetration guide or known attack, and would be large enough to warrant a massive scale architecture design and penetration test.

Auburn University's "Tigercard" system met all of these provisions. The Tigercard system at Auburn University is powered by CBORD group while the administration of the system takes place locally at Auburn. The cards are issued in the Auburn University student union. The dining facilities and many of the local businesses use Tigercards to allow students to pay for goods without the need for a checking account, credit card or other payment plan. Many of the soda machines on campus are wired with card readers to enable purchases to be made on the students' Tigercards.

Parents are capable of adding funds to the students' accounts online. Many of the new buildings, labs, and classrooms have key-card enabled locks that both control and log student and faculty access. Upon examination of the system, it was found that it uses a mix of both wired and wireless communication, varying levels of security, multiple hardware devices, and that the information was occluded from the public domain.

To begin looking at the Tigercard system we applied OSSTMM3's guidelines. The first step towards analysis requires that we define **assets** associated with the penetration tests. Based on card functionality, the vulnerable assets would be the card swipe door locks, the campus vending machines, and the networking equipment.

Our **scope**, or the channels from which penetration tests are derived, consists of three types. The *human* channel, represented by social engineering attacks, consist primarily of the Office of Internet Technology and the Office of Engineering. The *physical* channel is consists of the TigerCard, door locks and vending machines. The *data network* channel consists of the equipment, cables and the resulting information exchange.

Next, the controls are evaluated for limitations related to the assets. The first limitation, *weakness*, applies to the controls: authentication, resilience, subjugation and continuity. *Authentication* is utilized by the TigerCard system; however, it is only single factor as the card alone is sufficient for access and only exists on the physical level (i.e. possession of the TigerCard). *Subjugation* occurs on the physical level as the machine logs the use of the TigerCard; however, on the data network level, the data is unencrypted, allowing the receiver and not the provider to falsify identification. *Continuity* is not achieved as device failure results in a denial of service for most assets (door locks can have a key option but implementation is not universal). *Resilience* is not achieved on the data network level, as it is possible to swipe the TigerCard on a vending machine, disconnect it from the data network and then purchase an item without being charged. This is a known flaw, but the exact breakdown in the procedure that allows this in unknown. Because items vary in cost, the vending machine does not transmit the amount to be charged until after the choice is made. At this point the machine no longer has a connection by which to do so.

The second limitation, *concern,* applies to the controls: non-repudiation, confidentiality, privacy, integrity and alarm. *Non-repudiation* fails because authorization is only single-factor and requires something-you-have. Ergo, if someone steals or forges a TigerCard, no other checks are required to utilize the assets. *Confidentiality* and *Privacy* are moderately achieved via obscurity, as records of interactions are not displayed in the open; however, sniffing the traffic of the network may allow for the confidentiality and privacy to be completely exposed. *Integrity* is not established because a man-in-the-middle attack could alter the exchange of information without the knowledge of the victims. *Alarm* may or may not be weak. The authors do not know if records are kept of failed and disrupted transactions. If records are kept, it is not known if they are routinely reviewed.

In regards to the other two limitations, we have no known *exposures* or *anomalies*, though the latter may surface during the penetration testing process.
Vulnerabilities consist primarily in the *human* channel. A member of Office of Information Technology, Engineering Network Services, or friendly janitor giving access to the network closet or knowledge of systems internal workings would subvert the limited protections in place.

IV. The Plan

The plan to develop the penetration test was simple. OSSTMM3's penetration testing guide was followed

while at the same time utilizing the DoDAF architecture guide. This guide can be found on the main DoDAF repository, and was useful in gathering necessary system information and in constructing the DoDAF views useful for this test. Since this was a purely academic exercise there was no plan to attack or break the system in any way. The goal of the research was to gather as much information as possible as an initial test to the feasibility of the scheme. With this mindset the authors began gathering as much information from system as possible, being careful not to cause any damage or disruption, or to violate any sources of personal information.

Figure 1 – Lab Lock Photograph

Photographs were taken of the external hardware access points. This involved finding the connections for the vending machines and door locks, photographing them, analyzing how they might connect, and checking to see if the system functioned as speculated. With the larger system in mind we began to develop a rough outline of how the Tigercard system worked. Intelligence gathering was performed through the use if the Internet and search engines.

When a new piece of hardware was discovered it was photographed, and the manufacturer and part number recorded for review. An example of this is the card swipe locks on the lab doors. It was noted that the locks were Best Locks with card swipe readers. The part number was not visible. A single Google search revealed a wealth of readily available information. On the Best Lock site we were able to view several architecture diagrams, internal lock mechanism diagrams, and part numbers with feature lists for each of their products. This information made it clear how the locks operated within the confines of the Tigercard system. [3]

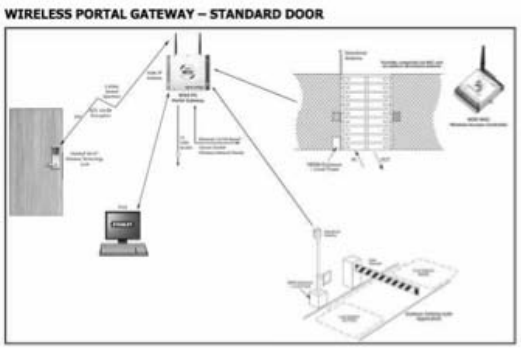

Figure 2 – Best Lock Diagram

It became onerous to gather additional information to perform a complete cyber penetration test. This information was grouped into several subcategories: what was being sent across the line, where it was going, and which format and standard of transmission was being utilized.

The Best Lock site gave us sufficient information to assume that door locks were controlled wirelessly, and a further inspection of the lock to our own lab confirmed this assumption. An inspection of the wiring to the vending machines led us to believe that Ethernet was being used to tap into the school network as part of the billing system. The wireless door locks seemed to be the least damaging or disrupting point for information gathering.

At this point, to try and get a better idea as to what traffic was being sent, we concluded that there were two fronts that we could use to attack the system. We could choose to sniff the wireless traffic to look for any unencrypted or easily breakable commands that would allow the door locks to be accessed, or we could sniff the Ethernet traffic to the vending machine to see what information was transmitted from the card and to see what the system response was that would allow a transaction to take place.

In investigating each of these options further it was decided that standard wireless sniffing equipment might be successful in obtaining the information that we needed to attack the door locks. For this purpose we would use WinPCap cards along with Wireshark to analyze the traffic over a period of time to try and isolate the traffic going to the doors to update the authentication system and to see what possible unlock and log information was transmitted.

To gain an attack vector on the wired door lock and the vending machine it was obvious that we would need to sniff the wired traffic being sent between the wired locks as well of the vending machine. To try this out we would need a passive Ethernet tap. After looking for a brief period several tutorials were found online. To test the

feasibility of this vector an Ethernet tap was built for less than twenty dollars in materials from Lowe's. [4]

Figure 3 – Ethernet Tap

Armed with these tools it was now possible to begin generating the initial architecture documentation and to develop the initial proposed series of test to evaluate the security of the Tigercard system.

V. IMPLEMENTATION

Several papers already exist on evaluating security on a complex system from DoDAF architecture. DoDAF has been criticized as lacking rigor from a security enterprise position. [5] However, previous work in using DoDAF as an information assurance architecture focused on the development of security policies in an attempt to rectify this deficiency, principally utilizing the OV-2, OV-5, OV-6A, and SV-1 views. [6] Penetration Testing relies on the same views; however, it focuses more on the disruption or exploitation of the security policy.

We began by developing the viewpoints for the DoDAF architecture in the order that was recommended by the architecture development section of the DoDAF repository. [7] The six-step process served as an excellent guide for modifying DoDAF to suit our needs. Through scoping our project and deciding what was relevant and what was known we were able to eliminate a good bit of the DoDAF architecture that would be needed or could be generated at this stage.

The All Viewpoints (AV) were useful for expressing the scope of what we intended to do with our project, and to justify our deviation from a traditional DoDAF architecture. The AV-2 was specifically helpful as it generated a standard dictionary for the purposes of synchronizing the terminology with the hardware and software companies that developed the system. This sort of insider knowledge is useful for future social engineering attacks, as it allows you to speak from a position of authority.

The Capabilities Viewpoints (CV) were of limited value as there was a lot of unknown information prior to the actual packet sniffing. We were unable to develop CV-1, CV-2, CV-3 or CV-4 without more detailed information of the inner workings of the system. This in itself was informative, as now the need to develop a method to gather this information was clear. In attempting to develop a way to gather this information we concluded that we could gain access to the networking closet to gain visual insight, discuss the issue with colleagues in OIT and at the student center that worked in administrating the Tigercard system, and by calling the support line at CBORD systems. CV-5 and CV-6 were successful in generating views from our idea of the required operational activities and the capabilities to services actions that were necessary. These would again be very helpful in discussing how the Tigercard system worked from a position of authority, and in verifying that our views of the system were correct.

The Data and Information Viewpoints (DIV) were useful in that we could use these as hypothetical models to try and form our penetration tests to gather lower level information of how the data must be formatted and shared. This is where more traffic sniffing would have to take place. Knowing that the information is on the Tigercard that every student is issued is very helpful in that it gives us at least part of the message being transmitted. A magnetic card swipe reader would be used to read that data, and to pinpoint the parts being sent to unlock a door or to make a purchase. The limiting factor was that we were only capable of creating a hypothetical DIV-1 dealing with the data and information at a high level. DIV-2 was decided as being not relevant for the purposes of our test, while DIV-3 would only be useful once we were able to sniff the traffic being sent to gain insight into the Physical Data Model. This would be very helpful, as it would contain the message format needed to gain access.

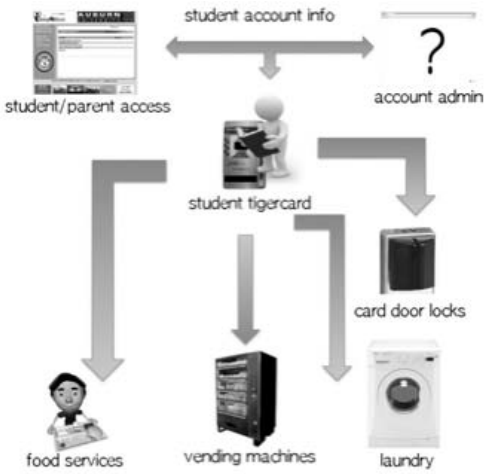

Figure 3- Example OV-1

The Operational Viewpoints allowed us to gain insight into how the system operated from a high level. This is where verification that we had a complete view of how the system works would take place. The OV-1 provided with the high level graphical concept that we could glean from interacting with the system as student, while more information will be needed to accurately fill in the OV-2 (Resource Flow), OV-3, OV-4 (Organizational Chart), OV-5 (Capabilities and Activities), OV-5B (Operational Activity), and finally OV-6c (Event Trace Diagram).

These remaining Operational Views are vital to the success of our penetration test, but in the lock of information that we have from basic information gathering we are able to determine an intermediate stage of penetration test that help to gain more information. In sniffing more traffic and targeting areas of social engineering we can more specifically define the information that we need to gain from individuals in order to complete our view.

As this was not a development project for us the Project Views were not required. These views would usually be used to show how the project would act in order to fulfill the need for which it was created. Generating these views would necessitate talking to one of the developers behind the system to determine the need that they foresaw and how they originally thought this system would fulfill the need of the customer.

The meat of the viewpoints, and where most of the useful information would come from for the purposes of penetration testing, would be filled in by the Services Viewpoints (SV) and by the Standards Viewpoints (StdV).

The Services Viewpoints would be used to generate the map of connections and the data flows throughout the system. These main documents would allow us to know where the information was flowing, and to map the weak points in the system. Unfortunately, due to our need to avoid damage and interruption at this point, we were unable to sniff the traffic and to follow the flow of information around the system. Foot printing and traffic sniffing would play a large role in gathering this information, and as such would be the logical next step for us to take.

Again, the lack of information in these two main view sets do help to guide our intermediate actions as to what information we would need to gather next. To fill out the SV-1 we need to ID the services and connections. We could do this by locating the wireless nodes and wired connection points throughout the building and using this as a map for how the rest of the system works. A proposed idea to finding this information was to use a spectrum analyzer such as Wi-Spy in order to determine the signal and location of the wireless nodes for the doors.

This could also aid in developing the SV-2, the description of resources and the resource flow. At the same time, while using the spectrum analyzer we can gather information about the wireless standard being used for communication. This identification of a standards whether it be 802.11 or 802.15 would allow us to generate to the standards view. Foot printing and listening on the wired traffic would also allow us to identify another standard which also aid in completing the Standards view.

The relationships of interest, namely the communication for the door locks and the billing system could then be identified, and the SV-3a, SV-3b, and SV-4 could be completed. The remaining views could then be drawn from the information gained in generating the previous views and the SV-7 matrix and views SV-10a-c could be generated to complete the outer view picture of the system.

Given this intimate knowledge of the inner workings of the Tigercard system the remaining effort would be spent in modifying an existing network attack or developing a new attack take advantage of a flaw in the flow of information or areas of weakness.

VI. Future Work

At this point our group has outlined areas where we need to gather more information on the Tigercard system in order to show how DoDAF and OSSTMM3 can be used to effectively provide a more scientific means of penetration testing and education about the security vulnerabilities which can be found in a system by simply looking around and asking a few people the right questions.

For our future work in this project we will be conducting tests to determine the format of traffic used, key points, the standards in place, and the message format. In gaining this information we will be able to complete the DoDAF views of the target system, and to generate a complete battery of penetration test, as well as to check the original design and network map of the system so that the system administrators can verify compliance with their own design and standards.

VII. References

[1] “Tech Stocks Set To Soar in 2011 as a New Era of Personal Computing Dawns - Money Morning.” http://moneymorning.com/2010/12/29/tech-stocks-soar-in-2011-new-era-personal-computing-dawns/.

[2] "New Hacking Tools Pose Bigger Threats to Wi-Fi Users - NYTimes.com," http://www.nytimes.com/2011/02/17/technology/personaltech/17basics.html?_r=1.

[3] "BestAccessSystems.com - Commercial security solutions provider for door locks and hardware, electronic access systems and key control." http://www.bestaccess.com/products/wiq.asp.

[4] "Create a passive network tap for your home network" http://thnetos.wordpress.com/2008/02/22/create-a-passive-network-tap-for-your-home-network/.

[5] Dalton II, M. G.C, D. R.J Colombi, and D. R.R Mills. "Modeling Security Architectures for the Enterprise."

[6] Hamilton Jr., J. A. "DoDAF-Based Information Assurance Architectures." *CROSSTALK* (2006).

[7] "DoDAF Architecture Development - 6 Step Process." http://cio-nii.defense.gov/sites/dodaf20/arch_development.html.

ISBN 1-933510-96-X/$15.00