Global Information Assurance Certification Paper

A Case Study: Information Assurance Testing During Operational Testing to Enhance Security of New Information and Data Exchange Systems

John M. Arnold, P. E.

Abstract

Enhanced connectivity and versatility of modern information and data exchange systems greatly improve accuracy and speed of communications. However, increased security risk comes with enhanced connectivity, and the Department of Defense (DoD) recently increased its emphasis on Information Assurance (IA) testing. For its part, the Army Test and Evaluation Command (ATEC) moved to enhance security of newly developed information and data exchange systems by incorporating IA testing into the operational testing (OT) of those systems. The bulk of IA testing is done as part of the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). In the past ATEC deferred to the DITSCAP for IA testing of new information and data exchange systems.

ATEC's recent move reduces overall security risk for new systems because the bulk of IA testing under DITSCAP is not done on fully-configured, production representative systems in realistic operational environments. IA testing under DITSCAP has generally been performed before systems "go live" in networks, and testing has been limited to identifying vulnerabilities with scans ("Blue Team" activity). Penetration attacks to exploit those vulnerabilities ("Red Team" activity) are deferred to a time when the system is fielded, a process that takes many months. By doing both vulnerability and penetration testing during OT, ATEC can assess the degree and extent of security risk associated with fielding of the newly developed system into its operational environment.

The Army's Distributed Learning System (DLS) was selected by ATEC as the first newly developed system to undergo IA testing during operational testing. However, military deployments and budget cuts caused the IA testing to take place during the all-up "dress rehearsal" test just prior to OT. This actually worked out well, and the IA attacker was impressed with the robust security features designed into the DLS Block 3 system. Still, the IA attacker was able to find and exploit some weaknesses, most notably when posing as a student inside a DLS Digital Training Facility (DTF). Using a student account, attacker was able to: 1. Alter test grades in a DLS learning application, and 2. Take control of a DTF workstation by installing Linux OS so it could be used to conduct attacks inside the DLS firewall. Extensive security features designed into the DLS architecture defeated other attack scenarios attempted. Interestingly, ATEC's results differed from DITSCAP results and are thought to be more representative of a "real world" outcome, primarily due to the comprehensive, system-level approach used. Overall, the DLS demonstrated robust security while delivering a wide variety of distance learning products to Army soldier-students worldwide.

A Case Study: Information Assurance Testing During Operational Testing to Enhance Security of New Information and Data Exchange Systems

John M. Arnold, P. E.

Introduction

US armed forces are continually developing, testing and procuring advanced weapons systems and other new technologies. Of the other-than-weapons-systems technologies, particular attention is being paid to new information and data exchange systems that combine Commercial Off-The-Shelf (COTS), Government Off-The-Shelf (GOTS) and newly-developed software to create complex, internet-based hierarchical networked systems that interface with other Department of Defense (DoD) and non-DoD systems. One such system is the U.S. Army's Distributed Learning System (DLS).

When fully deployed, the DLS will allow pre-registered soldier-students to take training and education courses virtually anywhere, anytime. Students can access courseware catalogs, select courses and take lessons online either at the home or office or at a DLS Digital Training Facility (DTF). The DLS operates 200+ DTFs worldwide to deliver training to students individually or in groups. Results of completed lessons are automatically posted to student training records, and student progress in achieving training and education goals is monitored in near-real time by training managers. To accomplish these and other "deliver and manage" training tasks, the DLS interfaces with several other systems. Two important interfacing systems are Army Knowledge Online (AKO) and Army Training Resource and Requirements System (ATRRS).

While this enhanced connectivity greatly improves the convenience and timeliness of training without degrading the quality, it also brings increased security risk. What if a disgruntled student attempts to change a lesson or course grade? What if hackers attempt a denial-of-service attack? What if a trusted insider seeks to disrupt operations? These and other Information Assurance (IA) risk issues must be mitigated prior to a new system being deployed. Such IA questions have been addressed in large part by the DoD Information Technology Security Certification and Accreditation Process (DITSCAP)[1].

The DITSCAP has three accreditation phases and one post-accreditation phase:

- Phase 1 objective is to establish the intended system mission, environment, architecture, security requirements, certification schedule, level of effort, and resources required for development and deployment of a new information system.

- Phase 2 objective is to produce a fully integrated system ready for certification testing.

- Phase 3 objective is to produce the required evidence to grant approval to operate the system; e.g., accreditation.

- Phase 4 post-accreditation objectives are to ensure secure system management, operation, and maintenance to preserve an acceptable level of residual risk.

Once a new information system achieves its accreditation under the DITSCAP, it can be fielded assuming all other-than-DITSCAP requirements for the system have been met as well. When a system is fielded it "ramps-up" to full deployment as iterations of the new system are produced and installed. Historically, it may take many months field a new system. All during this fielding process, the post accreditation DITSCAP phase, Phase 4, applies but no further IA testing is likely to take place until the system is fully-fielded or "mature".

The Problem

By law[2], an independent evaluation is conducted on production-representative samples of a new technology before the decision to purchase and deploy that technology is made. The Army Test and Evaluation Command (ATEC) has overall responsibility for independently evaluating new technologies to determine their effectiveness, suitability and survivability upon deployment. In the past ATEC deferred to the DITSCAP for IA assessments of newly developed information and data exchange systems. However, accreditation under DITSCAP occurs during the late stages of development, prior to providing a production representative system for ATEC to evaluate in a realistic Operational Test (OT) environment. IA testing for accreditation has generally been limited to identifying vulnerabilities with scans (so-called "Blue Team" activity). Penetration tests - i.e. staging penetration attacks to prove the degree of risk of those vulnerabilities (so-called "Red Team" activity) - are not performed very often as the system has yet to "go live" in a real-world networked environment. By doing both vulnerability assessments and penetration tests in a real-world network environment the degree and extent of risk associated with deployment of the newly developed system can be fully quantified and understood. OT is conducted in such an environment and is the last major test and evaluation hurdle prior to the government decision to purchase and deploy the newly developed system.

Recent events[3] have underscored the importance of conducting IA testing as part of OT to obtain the most realistic security risk assessment possible on a new system before fielding that system. All branches and agencies of the Federal

Government, including the Army, have recognized that attacks on information and data exchange networks are escalating just as the reliance on those systems is escalating. Newly deployed systems can be particularly vulnerable to attack because IA testing under Phase 4 post-accreditation may not take place until ramp-up is nearly completed many months after the fielding decision is made.

The Solution

Recently in a coordinated effort, ATEC's Information Technology Evaluation Directorate (ITED) and Command, Control, Communications and Computers Test Directorate (C4TD) conducted the first IA penetration test during operational testing of a new information and data exchange system. In June-July 2003 the Block 3 enhancement to the Distributed Learning System was operationally tested starting with an all-up, full-system End-to-End (E2E) test. During the E2E, IA testing was also conducted. The selected IA testing agency was the Information Systems Engineering Command (ISEC). ISEC had previously conducted an IA assessment of the DLS Block 3 enhancement to fulfill the DITSCAP requirement for accreditation. This previous work by ISEC provided an opportunity to compare results obtained using both approaches, and it identified ways to refine and harmonize the two approaches so unnecessary duplication could be avoided.

Implementing the Solution

Test Planning. Prior to the E2E/OT, IA testing requirements were prepared for the selected IA testing agency to follow in conducting the test during OT under ATEC's auspices. Limits were designed into the IA testing requirements to preclude harm to existing networked systems. While the test requirements were in preparation, a process was also underway to select the appropriate IA testing agency. Selection of the IA testing agency initially centered on the 1st Information Operations Command (1st IOC). 1st IOC is the Army's only authorized agency to conduct penetration testing on "live" networked information and data exchange systems[4]. However, with the nation committed to warfighting operations, the resources of 1st IOC were unavailable during the planned test "window". 1st IOC did consent to participate in an advisory role and assisted in structuring the initial IA testing requirements.

Based on 1st IOC's unavailability, ATEC solicited participation from ISEC as the IA tester during OT. ISEC had just completed a vulnerability assessment of the DLS Block 3 as part of DITSCAP certification requirements. This was seen as a plus in planning and executing IA testing during OT.

Test Design Considerations. Test design benefited from the work already done as part of DITSCAP and focused on what disgruntled students might do to

change grades, disrupt operations and acts of similar nature. These are very valid events that most likely will sooner or later happen in the Distributed Learning System where results become a permanent educational record.

One purpose of ATEC's evaluation is to assess the ability of DLS users (students, system administrators, or others) to recognize and respond to an attack on the DLS. Another purpose of ATEC's evaluation is to determine whether or not users are adequately trained to respond to an attack regardless of where the attack came from inside or outside the DLS firewall. These "recognition and response" scenarios have nothing to do with the vulnerability (or invulnerability) of the DLS considered by the DITSCAP. The evaluation will fit any information system regardless of its use. The DITSCAP process assessed the system's intrinsic vulnerabilities. Now the IA assessment needed to be extended during OT to determine if representative users can still use the system when confronted with an attack.

ATEC's evaluation has two parts. The first part is assessment of the vulnerabilities. The second part is the human aspect, both from the attack perspective and from the unknowing user perspective: someone who may or may not experience difficulty with the system when an attack is underway. It is therefore necessary to design a test that will challenge the users and their ability to recognize and respond to the attack.

As Figure 1 shows, the DLS Block 3 system is comprised of several subsystems - highlighted in yellow - and interfaces with existing Army systems (legacy systems). Of particular importance to the DLS Block 3 are the Army Knowledge Online (AKO) and the Army Training Requirements and Resources System (ATRRS) interfaces shown on the upper left-hand portion of the diagram.

Soldier-students - or courseware quota managers if an entire class is to be scheduled for a group of soldiers - must use the ATRRS courseware library to select, register and schedule delivery of course lessons. ATRRS also keeps track of student progress through course lessons or modules, records test grades, course completions, and maintains transcripts as part of soldiers' official training records.

To utilize the DLS Learning Management System (LMS), the student first visits the Internet and enters the AKO portal. The student then navigates into the DLS LMS site where courseware can be searched via the ATRRS courseware library link and then selected and distributed to the chosen DTF or remote location on the date needed. The far right of the DLS architectural diagram shows the DTFs where soldier-students come to take courses delivered to them by the DLS system. Since the DTFs operate inside the DLS firewall, a focus of the IA planning was the networked student workstations within the DTFs.

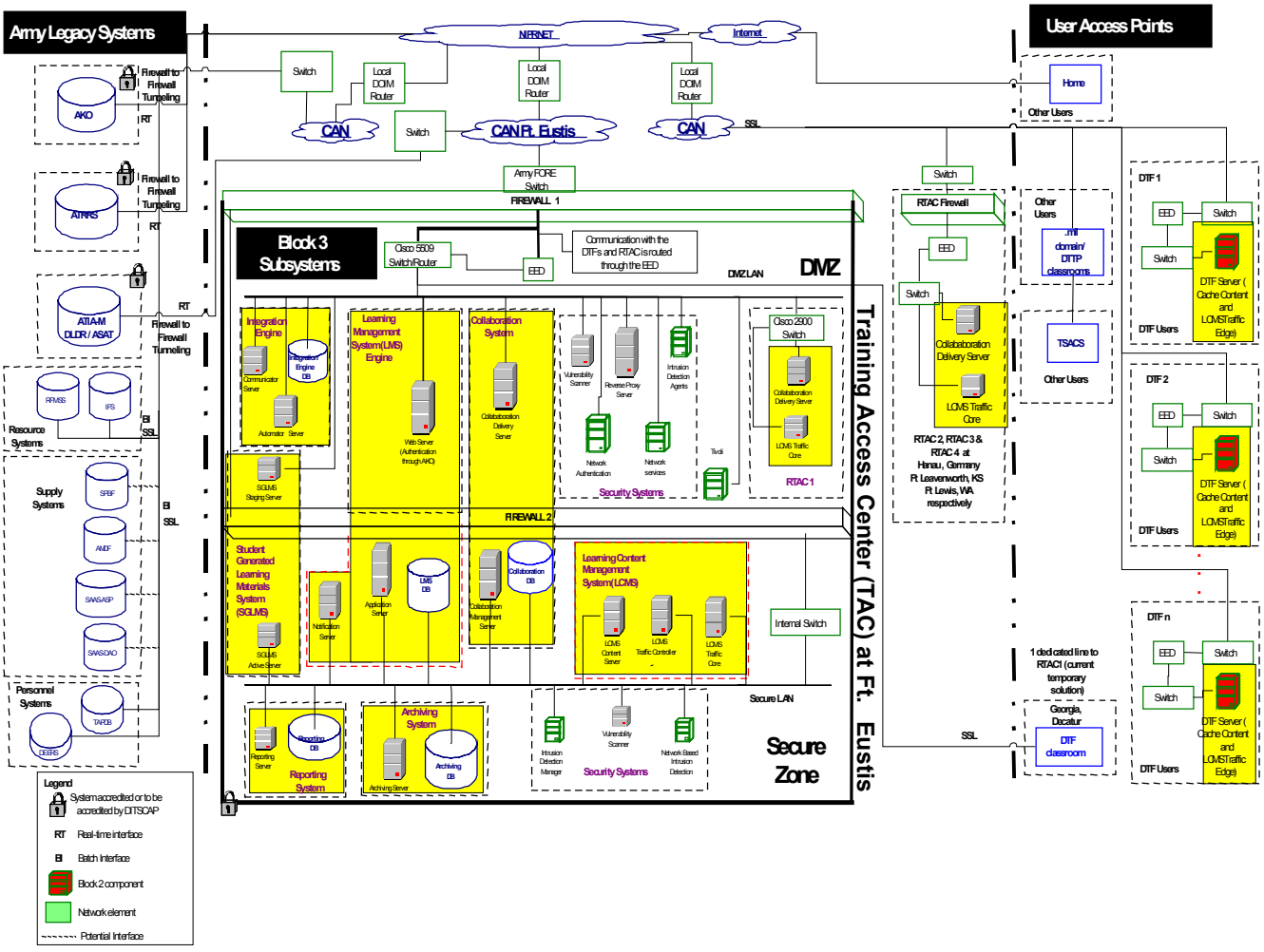

Figure 1. Distributed Learning System Block 3 Architecture[5].

Scenarios Planned. From the test planning process, eight attack scenarios were created and four were ultimately selected along with three "recognition and response" evaluations for a total of seven test cases. While the details of the plan are not public information, the original eight attack scenarios from which the test cases evolved are:

- Disgruntled student wants to change test results.
- Unauthorized person wants to gain access to sensitive course materials.
- Disgruntled student wants to disrupt classroom.
- Disgruntled user wants to disrupt operations.
- Disgruntled student wants to modify and embellish their training record.
- Unauthorized person wants to take DLS courses. From outside the .mil domain.
- Authorized user wants to create a DLS System Administrative account.
- Disgruntled user wants to delete entire sections of the DLS database architecture.

The Results

Military warfighting deployments and budget cuts in support of those warfighting deployments prompted a reduction in scope and testing dates were accelerated so IA testing could take place during the all-up, full system End-to-End (E2E) "dress rehearsal" test conducted just prior to entering the OT. This section of the report gives a snapshot of the IA testing conducted and the preliminary results obtained.

Test Execution. The test team attacked the system against seven security-related test cases derived from four of the eight original attack scenarios and three associated "recognition and response" scenarios, namely:

- Disgruntled student wants to change test results.
- Unauthorized personnel want to gain access to sensitive course materials.
- Disgruntled student wants to modify and embellish their training record.
- Authorized user wants to create a DLS System Administrator (SA) account; using security automated tools to identify vulnerabilities that could be exploited by a “hacker”.
- Attacker wants to determine if the DLS implemented approved security tools to audit and alarm security officer.
- Attacker has already penetrated the DLS firewall and wants to determine how system administrator recognizes and responds to an attack.
- Attacker wants to evaluate the ability of the system administrator and/or

security manager to recognize and respond to an attack on the DLS firewall.

Security Tools Utilized. Considering the scenarios identified above, the test team considered the attacker to be on a limited budget and performed a series of Internet searches by utilizing the GOOGLE[6] search engine to find security tools readily available as downloads for evaluation purposes. The tools selected were:

- GFI LANguard[7]: Network scanning tool.
- Internet Security Scanner (ISS)[8]: Internet scanning tool.
- LOphtCrack[9]: Password cracking tool.
- Knoppix[10]: Linux OS bootable CD.
- AppDetective[11]: Oracle and MS SQL scanning tools.

Test Findings. The test was divided into two phases and all seven test cases were tested against the system at each phase. The first phase was to attack the system behind the DLS firewall. In the second phase, the test team tried to penetrate the system from outside the DLS firewall. The following paragraphs discuss each test case and its findings. Each paragraph includes the reference number extracted from the security scenarios and the discussion of the test result.

Test Case 1 (Attack Scenario 1): Disgruntled student wants to change test results

Here attacker sought to determine if the DLS has implemented security to protect the system from unauthorized access. This test case was conducted both inside and outside of the DLS firewall. When inside the DLS firewall, attacker succeeded in changing test grades, which shows a student can modify test results before submitting those results into permanent records. While the problem uncovered did not relate to any system security vulnerability, it revealed a design flaw in the DLS courseware application being used. The courseware manager was advised that the "Current Score" option should be made inactive or removed to prevent a student from entering a score and percentage of completion for a particular test or courseware lesson.

Test Case 2 (Attack Scenario 2): Unauthorized user wants access to sensitive course material

Here attacker sought to determine if the DLS has implemented security to protect the system from unauthorized access. This test case was conducted both inside and outside of the DLS firewall. When inside the DLS firewall, attacker with a normal soldier-student account logged on at a DTF student workstation and downloaded from the internet evaluation copies of AppDetective database scanning software applications to match Oracle or Microsoft Structured Query Language (SQL) servers to DLS internet protocol (IP) addresses. Attacker failed when password access the DLS LMS database could not be defeated.

Test Case 3 (Attack Scenario 5): Disgruntled student wants to modify/embellish training records

Given enough time to hack a system, an attacker will sooner or later penetrate that system. However, attacker found that access to the DLS servers and databases is not a simple task. The multiple layers of defense such as password protection and intrusion detection system (IDS) safeguards coupled with operating system (OS) security measures and strict firewall policies made this an impossible avenue of successful exploitation given the limited time to mount the attack. Nevertheless, due to a design flaw in the software application, attacker was able to choose his own final score and then enter it into his official record (see Test Case 1).

Test Case 4 (Attack Scenario 7): Authorized user wants to create a System Administrator account

Here attacker began with a valid soldier-student account and attacked from inside a DTF at a student workstation. Attacker attempted to access server from "my network neighborhood" and "map network drive". Since all student workstations in the DTF are behind the DLS firewall, attacker is able to see the systems on the same domain but is not normally able to access them. In order to use network mapping where network shares are password protected, attacker must know the specific shared drive name and valid account with appropriate access rights. In addition to using the LopthCrack password cracking tool, attacker attempted to connect to the network mapped drive using the administrator account and guessed passwords, but was not successful in cracking the administrator password due to "time out" security discipline. One student workstation attacker used during the test was found not to have its BIOS setup correctly. Therefore, attacker was able to boot that system from a CD that contained a LINUX OS and then took control over that workstation as system administrator. Setting the system BIOS to boot up of the workstation from "C" drive easily mitigates this problem only. It was learned that when a recent Windows OS upgrade was performed the BIOS was changed to permit boot up from the workstation CD drive. Security procedure required the BIOS to be returned to baseline (C drive boot up), but this was not done. Once the Linux OS replaced the Windows OS, control - and therefore security - of that workstation was compromised. System was now vulnerable to exploitation by breaking admin account/password at the server level.

Test Case 5 (Recognition/Response to Attack Scenario 1): Attacker wants to learn if the DLS deployed an Intrusion Detection System

This test case was conducted inside and outside of the DLS firewall. Here attacker used LANguard software and ISS automated tool to exploit system vulnerability from behind the firewall. However, the deployed IDS alerted EMC

security manager and the scan port was closed to stop the penetration. Attacker was unable to penetrate the system from the outside the DLS firewall using the same tools.

Test Case 6 (Recognition/Response to Attack Scenario 2): Attacker has already penetrated the DLS firewall and seeks to determine how the DLS reacts to an insider's attack.

Test Case 6 was conducted at the Internet protocol (IP) network level. Here, as in Test Case 4, attacker was unable to access the DLS server using network mapping since all network shares were password protected. In order to use network mapping, attacker must know specific shared drive name and valid account with appropriate access rights. Attacker also failed to access the server using telnet sessions. Attacker used LOpthCrack password cracking tool but was unsuccessful in cracking the administrator password to gain control. Since audit trail logs capture all failed logon attempts, the SA was able to identify the attack and report it to security manager for his appropriate action according to the DLS security policy.

Test Case 7 (Recognition/Response to Attack Scenario 5): Attacker seeks to determine the system administrator and/or security manager to recognize and respond to an attack on the DLS system.

Once the DLS system administrator and/or security manager received alarms from IDS, the DLS SA/SM quickly assessed the situation and blocked the intrusion attempt.

Conclusions and Recommendations

ATEC's Information Assurance test team concluded that the Distributed Learning System has implemented all available security measures and countermeasures to protect the system from penetration attacks. The attacker found multiple layers of defense-in-depth coupled with the OS security measures and closed ports by default firewall policies. These measures made the DLS a very unlikely avenue for successful exploitation. While no system that can be called a perfect system when it comes to security, the DLS was found to have one of the most robust security systems in its class. Deficiencies found were due to: 1. A design flaw in the LMS's adminstration of courseware applications that permitted grades to be changed prior to submitting them to the permanent record database; and 2. Personnel noncompliance with established security procedures when changing or upgrading a DTF workstation OS.

The ATEC IA test team recommended that DLS management change the LMS administration of courseware to remove the design flaw and improve security training procedures to minimize or eliminate the vulnerabilities identified.

List of References/URLs

[1]DoD Instruction 5200.40, 30 December 1997.
[2]Public Law 92-156 enacted 1971.
[3]Morrow, Lance, "The Case for Rage and Retribution" Time Magazine, Vol. 158, No. 12, 14 September 2001.
[4]DoD Directive 5200.28, 21 March 1988.
[5]ATEC Event Design Plan for the Distributed Learning System (DLS) Block 3 Initial Operational Test (IOT), April 2003.
[6]GOOGLE search engine, URL: http://www. google.com.
[7]GFI LANguard download site, URL: http://www.gfi.com/.
[8]Internet Security Scanner (ISS) download site, URL: http://www.iss.net.
[9]LOphtCrack download site, URL: http//www.astaserials.com.
[10]Knoppix download site, URL: http://www.knoppix.org.
[11]AppDetective download site, URL: http://www. appsecinc.com.