Reinforced Plastics

ISSN (online): 0034-3617

Adaptive Hierarchical Cyber Attack Detection and Localization in Active Distribution

Vanapamula Veerabrahmachari, Arekatla Madhava Reddy, Dr. G. Samba Siva Rao,

Dr. Padigala Suresh

[1,2] Assistant Professor, [3,4] Professor

vveerabrahmachari@gmail.com, amreddy2008@gmail.com,

profgssrao@gmail.com, padigalas36@gmail.com

Department of CSE, A M REDY MEMORIAL COLLEGE OF ENGINEERING AND TECHNOLOGY,

PETLUVARI PALEM, ANDHRA PRADESH-522601

Abstract

Unlike dangers such as radioactivity that have always been a part of space travel, a malevolent and enduring threat can change over time. As a result, conventional systems engineering methods and models may need to be extended or modified to successfully handle the more dynamic behavior and uncertainty of modern mission systems.intelligence-based features of one's opponent. This document details the implementation of a typical espionage assault against mission systems that have been "secured" in the conventional sense, such as by being in accordance with the standard IT Security Plan. By analyzing a real-world assault in the context of a task, we were able to pinpoint the most pressing issues in need of systems engineering attention moving forward. In particular, initiatives that seek to fortify mission systems against the online enemy. In brief, the basic espionage example given here shows how a group of "secure" computers can be constructed into an unsecure system, highlighting the need to investigate cyber-defensive testing infrastructure, methods, and toolkits, as well as the ways in which these can be connected to testing objectives.

1.Introduction

Motivation

Protecting valuables in space from the harsh conditions of space is essential. As with radiation bands and temperature anomalies, cyberspace attacks can be shown to be just as damaging to satellites and their ground-based data and support systems. Openly documented instances of hostile hacking behavior targeting space objectsAmong the relevant material is the following: "On July 23, 2008, Landsat-7 encountered 12 or more minutes of disturbance. The accountable entity did not complete all necessary procedures for satellite control. There was interruption for at least nine minutes on October 22, 2008, on Terra EOS AM-1. All conditions for commanding the spacecraft were met, but no orders were issued by the accountable entity. In December of 2010, Chinese officials arrested a Chinese citizen for allegedly breaking Chinese Administrative Law. This is the first time a Chinese citizen has been arrested for breaking into U.S. government networks. The Chinese citizen gained unauthorized access to seven NASA networks, many of which contained sensitive technological information that could not be exported.2 "A Romanian national known as "Tink ode" pleaded guilty in a Romanian court in June 2012 to charges of illegally accessing numerous systems belonging to NASA, the Pentagon, the Romanian government, and U.S. commercial entities."3 "...a computer virus recently infected the ISS."4There is no shortage of warnings and cautions. The US DNI ranked "cyber" as the top danger to the US in 2014, and he warned that threats to US space services would rise in the coming year and beyond as possible foes sought out disruptive and damaging counterspace capabilities. Military officials in China and Russia are aware of the informational benefits offered by space systems and are working to create the means to counteract American use of space during combat. For instance, official Chinese military documents stress the importance of disrupting, damaging, and destroying spacecraft used for surveillance, guidance, and communication. China can disrupt satellite signals and is developing anti-satellite technology. In 2007, China destroyed its own spacecraft in an anti-satellite test. Space security is regarded as an integral part of Russia's national defense according to the country's 2010 military policy. The Russian government has been very transparent about

the existence of antisatellite weaponry and related studies. Both satellite jammers and anti-satellite devices are in development in Russia.5

Goals

The purpose of this study is to determine if security defects in a sample mission system can be uncovered by employing a collection of key system engineering principles for V&V (Verification and Validation) testing.In Section 2, we outline the essential components of a successful V&V campaign, and in Section 3, we examine connected endeavors in the area of security testing. In Section 4, we'll look at an example mission system that has been determined to be "secure" by meeting all of today's standards for digital safety. We then apply the V&V characteristics to the system and describe in depth a real-world espionage assault that we conducted with great success.We present our findings from the testing, talk directions for future research, and draw some final inferences.

2. Technical Approach

Concerns with conventional System Engineering testing range from the security of the systems being tested to the training of test team members. We limit our attention in this article to the following primary issues: Validation, verification, and evaluation on your own time. We believe these to be the most important factors to consider when providing evidence that a method istrue safety.JPL has extensive expertise with automated failure prevention for flying missions, and our team is bringing this knowledge to the discovery, analysis, and mitigation of cyber-attacks as part of our work to adapt to the changing threat landscape. However, testing the limits and mitigations is necessary for developing and deploying effective countermeasures. The V&V program is the traditional capstone of test engineering; it answers the question, "Does the system perform as the system engineers intended?" Does the implementation deliver the expected results? This new strategy calls for specialized testing in cyber protection to precede the standard V&V effort.

Independent Review

Reviewing specialists have an inherent predisposition toward a positive outcome, and they are led in their assessment by the system's practical requirements. An external party should check if a system can be tricked into doing something it wasn't designed to do by exploiting known vulnerabilities.not committed to the functionalist worldview.

Validation

The effectiveness of cyber defense plans against the assaults they are meant to prevent requires validation in a practical setting. The process of approval raises consciousness and comprehension of its robustness in the face of a relentless and changing foe. Knowing which systems could malfunction and in what circumstancesthe certification procedure entails determining the failing circumstances and devising a plan to overcome them.

3. Related efforts

It's not a novel concept to try to improve computer security with more rigorous, organized methods. After introducing "The Specification and Modeling of Computer Security"7 in 1990, McClean took a retrospective look at his work bringing structured techniques to cyber security testing nine years later.8 JPL colleagues have carried on with this concept.for the purpose of protecting software while it's being created and while it's being updated.9USC researchers have made great strides thanks to the DHS/NSF-funded DETER project, which aimed to provide "fundamentally transformational cyber security research methodologies" by going "beyond the classic 'testbed' model."10 Suites of tools like SEER (Security Experimentation Environment)11 and Montage12 aim to reduce human mistake by centralizing and standardizing as much of the experiment's life cycle as possible.Recently, we have been conducting trials in cyber security using preexisting testbeds like DETER. Overall, we've found that most of these systems offer novel ways to handle cyber security testing, but rarely follow through on those claims beyond the proof-of-concept stage. However, it is uncertain from a public viewpoint what may be accessible in this domain because we have not dealt with more restricted access testbeds like the DHS NCR (Department of Homeland Security National Cyber Range)13.Our present focus is on constructing a CDRL (Cyber Defense Research Lab) that can federate with other existing testbeds and begin implementing our suggested new testing strategy. Our initial procedures were very similar to those outlined in the "Penetration Testing Lab"14 written by the Rapid7 Metasploit team.

4. Deploying and Understanding an Attack

As part of a "Reconnaissance demonstration," an exploit in the security system was frequently tested. This demonstrated how a determined attacker could

take advantage of a lapse in security and carefully probe the rest of an organization's systems.

Test Infrastructure

We made an almost exact replica of a mission design in the actual world. The standard security tests, such as vulnerability assessments, had been performed, and found no issues with that design. Dev, Test, and Ops were the three sections of the system. (Development, Test, and Flight Operations). All three were surrounded by the company perimeter firewall, and Ops was protected by yet another firewall/bastion-host. (See Figure 1).For this exercise, we used a testbed consisting of some computers, a cheap 8-port ethernet gateway, and some recently retired PCs from a space program. (Virtual machines). In order to segregate the other computers and track network activity, we used a dedicated physical server as a conduit between our trial and the company network. It was safe to perform tests without worrying about accidentally disrupting the simulated task machinery.

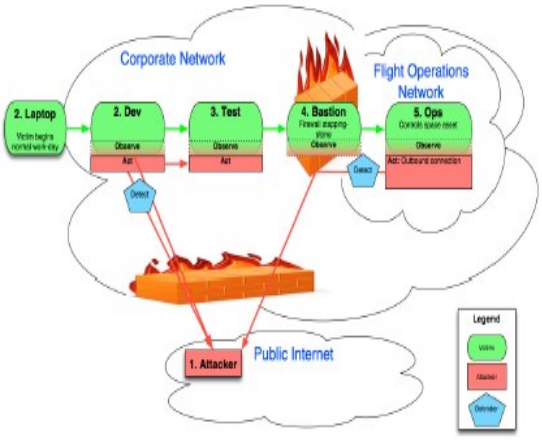

Fig. 1.Recon Roadmap

Run Attack, Observe Consequences

A number of people played roles in the "Reconnaissance demonstration," including the aggressor, the sufferer, and the defense. In total, there were six stages:First, an intruder gains write access to a victim's personal location with only one syllable of the victim's password.to get things done. As a result, the intruder was denied entry. Imagine approaching a victim's notebook in a public place like a coffee establishment.Our target then proceeded to do some routine office work:Utilized a login, password, and one-time-use code with a personal identification number (PIN) to log into the development environment. This verification creates a single sign-on (SSO) pass that can be used to access multiple computers without having to go through the multi-factor procedure again.

Third, I switched accounts from Dev to Test using the SSO request.Fourth, connected the Test server to the Ops base host via the firewall. Since the SSO confidence did not carry over to the Ops environment, we had to go through the multi-factor login process again.Connected to an Operations workstation.Six, I signed off of all devices like I was leaving for the dayFollowing the original intrusion, which took less than a minute, the assailant could monitor the victim's every move and assume unilateral control of any computer the target used. The perpetrator had complete, continuous access to all three settings by the time the target was done. But our guard had seen something strange.

Reconnaissance Scope

The goal of our development was not to create assaults that are easy to counter. We didn't bother trying to be covert because any actual user could have easily spotted the perpetrator. Due to our foreknowledge of the victim's actions, the assailant failed to account for other plausible real-world situations.We put the simulator through its paces using fictitious alerts and messages.

Initial Breach Attack Tree

Many real-world instances of the first stage of a compromise have been thoroughly documented. The possible protections are depicted as blue shields in Figure 2's tiny attack tree, with "victim goals" in green ovals and "attacker actions" in red squares. We checked the plausibility of the situation by walking through several real-world instances of distant breaches of (older)software very close to what can be found on mission development computers (web servers, databases, etc.).

Fig. 2. Attack Tree

5. Observations and Results

Test as you fly, fly as you test

Systems and equipment typical of those used for space flights were put through their paces in the scouting display. All of these pieces of hardware and software are protected by standard IT safeguards, have been through non-intrusive vulnerability assessments, and are managed by configuration control. The framework and supporting apparatusas part of this comprehensive evaluation, all security measures were kept unmodified. For this reason, it's important to simulate the production setting as closely as feasible during testing.The demonstration revealed that there were significant holes in coverage across the combined system, which meant that alerts were often wrong in their reliance on underlying systems. Designs for monitoring that were comprehensive when viewed from a single layer and viewpoint often required additional testing and validation to ensure full coverage when used in conjunction with other systems. The accepted but unproven stance was that each layer of control was already giving the necessary security, but when these powers were joined, a new danger emerged that had never been examined, tried, or approved before. Through this display, we were also able to pinpoint areas where insufficient preventative measures had been put in place and where the real threat to operations had never been discussed.

Fault containment aligned with lifecycle management

The events brought to light the fact that the actual fault confinement zones were not as effective as people had thought they would be. The mission-supporting systems and the security measures they employ can be broken down into three categories following the typical systems development lifecycle:

Check, and Function. The security flaw in the example was in the testing system, which allowed the attackers to gain access to the single sign-on function.Existing security controls were found to have coverage holes during testing and presentation, leaving the Test and Operations environment vulnerable to threats from the Development environment.Unfortunately, development environment controls are not always as stringent as Test and Operations controls. If an attacker can exploit these management flaws, they may be able to move on to the other, more secure settings, as demonstrated here.

6. Future Work

We are trying to implement a thorough approach and toolkit for reproducible testing of cyber security solutions, drawing inspiration from JPL's expertise with spacecraft V&V operations. Metrics for contrasting "normal" with "abnormal" system behavior and for measuring progress toward goals are currently under development.phase tests that contrast systems before and after mitigation.Concurrently, we are developing a unique testbed for cyber protection. Such a testbed would allow us to achieve our goals of high-fidelity system capture, repeatability, and automated capture of real-time state for generating metrics, in addition to considering traditional features of a cyber-security testbed like sanitization between experiments, isolation, and strong access control.

Testbed Connectivity

We have determined requirements that correspond to different (incompatible) degrees of network accessibility: Completely sealed off for dealing with active infections Locked down firewalls for the few external services we use that we can't build ourselvessuch as a designated identification system, point-to-point tunneled, like DETER lab (see below), open to the company network, and open to the Internet are all viable options.There is still work to be done on developing the methods for delivering these and making the transition between them without incident. Particularly difficult is making sure that any malicious software tested in complete isolation is completely eradicated before reintroducing users.

7. Conclusions

Our preliminary experiments show that, despite the usual security checks, modern systems are not ready for the cyberattacks of yesteryear. Cyber protections can be verified and validated more thoroughly by employing system engineering processes in addition to IT conformance checks.We saw a wide variety of assault methods successfully breaching systems in a variety of settings. Many people expected standard measures to impose error confinement as a cyber security remedy, but this did not happen. This finding highlights the importance of V&V procedures that can deal with flexible, evolving dangers.We saw how building choices can have unintended results, such as user-friendly system elements actually aiding the enemy. SSO (Single Sign-On) specifically allows the user to access everything associated with their name with a single login. A better solution than blindly believing a coarse-grained peripheral firewall is to raise awareness and instruction about this occurrence, which

emphasizes the need for application-level security, where each component shields itself from the others.Weaknesses in the architecture could be easily seen thanks to the test setup. It's important to simulate component relationships as closely as possible without putting live systems at risk.

References

1. U.S.-China Economic and Security Review Commission, "2011 Report to Congress", p. 216 (p. 224 of the PDF) http://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf

2. Martin, Paul K., "NASA Cybersecurity: An Examination of the Agency's Information Security", Testimony before the Subcommittee onInvestigations and Oversight, House Committee on Science, Space, and Technology, U.S. House of Representatives, Statement of theInspector General NASA , 2012-02-29, p.8 (p.9 of the PDF)http://oig.nasa.gov/congressional/FINAL_written_statement_for_IT_hearing_February_26_edit_v2.pdf

3. NASA OIG "Semi-annual report", April 1 - Sept 30, 2012, p.23 (p.29 of the PDF)http://oig.nasa.gov/SAR/sar0912.pdf

4. NASA OIG memorandum, "NASA's Most Serious Management and Performance Challenges", November 10, 2008, p.15 (p.19 of the PDF)http://oig.nasa.gov/NASA2008ManagementChallenges.pdf

5. Clapper, James, Director of National Intelligence, "Worldwide Threat Assessment of the US Intelligence Community", Statement for theRecord, Senate Select Committee on Intelligence, January 29, 2014, p. 7 (p 11 of the PDF)http://www.dni.gov/index.php/newsroom/testimonies/203-congressional-testimonies-2014/1005-statement-for-the-record-worldwide-threatassessment-of-the-us-intelligence-community

6. NSTAC (The President's National Security Telecommunications Advisory Committee) "Report to the President on Commercial SatelliteCommunications Mission Assurance", p. 18 (p. 28 of the PDF)http://www.dhs.gov/sites/default/files/publications/NSTAC STF Report FINAL 11302009_0.pdf

7. McLean, John. "The Specification and Modeling of Computer Security" IEEE Computer 23 , no. 1 (1990): 9-16. http://www.dtic.mil/dtic/tr/fulltext/u2/a462368.pdfhttp://www.bibsonomy.org/bibtex/25355027356c7985cc770b112ee9f64f5/dblp

8. McLean, John. "Twenty Years of Formal Methods" Paper presented at the meeting of the IEEE Symposium on Security and Privacy, 1999, p.115-116. IEEE Computer Society, (1999) http://www.cs.washington.edu/research/projects/poirot3/Oakland/sp/PAPERS/S04_05.PDFhttp://www.bibsonomy.org/bibtex/2334022333b477e1fb8fda4d71c1c33a1/dblp

9. Gilliam, David P., Powell, John D. and Bishop, Matt. "Application of Lightweight Formal Methods to Software Security" Paper presented atthe meeting of the WETICE, 2005. http://trs-new.jpl.nasa.gov/dspace/bitstream/2014/41246/1/05-0737.pdf http://www.bibsonomy.org/bibtex/2c9a5b901837f474c0d566624ff088704/dblp

10. Benzel, T., Braden, B., Faber, T., Mirkovic, J., Schwab, S., Sollins, K., and Wroclawski, J. "Current developments in deter cybersecuritytestbed technology". Proceedings of the 2009 Cybersecurity Applications & Technology Conference for Homeland Security (Washington,DC, USA, 2009), CATCH, IEEE Computer Society. http://www.isi.edu/~mirkovic/publications/catch-deter.pdf