ANTI-TAMPER TECHNOLOGY: PREVENTING AND/OR DELAYING EXPLOITATION OF CRITICAL TECHNOLOGIES

by

Christopher L. Cain

A Capstone Project Submitted to the Faculty of

Utica College

August 2013

In Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Cybersecurity

Abstract

United States military technology can be compromised, exploited, and reverse engineered through various means. Military technology is susceptible to foreign sales, accidental loss, and capture. It can be disabled on the battlefield, and is vulnerable to espionage. United States military assets provide a superior technological advantage and therefore require priority protection against these risks. Members of the Department of Defense, including civilians and contractors, can mitigate these risks by understanding and implementing priority protections known as 'Anti-Tamper'. With the ever changing requirements and advancements in technology, Department of Defense Anti-Tamper policies and procedures must be adhered to and updated continuously. These Anti-Tamper policies not only explain how, when, and where to integrate these Anti-Tamper protections, but also how to feasibly integrate them into the weapon system's life cycle.

The quintessential performance of Anti-Tamper technology is made possible through software watermarking and fingerprinting, encryption wrappers, hardware-assisted protections, and code obfuscation. Because of the advancements in technology, the U.S. military can continue to provide protection to a plethora of sensitive classified information that would otherwise degrade tactical ability as well as unwarranted proliferation of costly weapon systems.

Keywords: Cybersecurity, Professor Christopher Riddell, acquisitions, countermeasures, exploitation, intelligence, critical.

Acknowledgements

The path to enlightenment is paved with the question ‘Why’. I would like to dedicate this thesis to my little inquisitive minds: Carter and Jennavieve. May knowledge and truth always be in attendance for you to grasp upon and capture. May your hearts be full of excitement and your eyes full of wonder. It is my solemn pride and accomplishments as a father to witness both of you grow into your own. May technology continue to promote enlightenment and freedom for both of you and the generations to come.

I would like to praise my wife Emily for her unrelenting devotion and illuminating character. Her patience, support, comforting words, and soothing disposition made this all possible.

I would also like to show appreciation to my Professor and Capstone Chair, Christopher Riddell, my second, technical reader, Professor Joe Giordano whose patience and guidance were always welcomed throughout the Utica College Cybersecurity M.S. Program.

Table of Contents

List of Illustrative Material

Anti-Tamper Technology: Preventing and/or

Delaying Exploitation of Critical Technologies

Throughout history, adversaries have adapted, and overcome technological obstacles during both war and peacetime. During the past three hundred years, the United States (U.S.) military has grown from a newly formed fighting force made up of farmers and minutemen into a sophisticated military construct. The advanced technological integration between man and machine has the potential for extensive vulnerabilities. The existence and exploitation of these vulnerabilities have created the need for Anti-Tamper technology (AT).

Battlefield losses are inevitable; however, the advancement in military hardware has contributed to the decrease in casualties over the last twelve years. Since 2001, casualties of the Iraq and Afghanistan war have exceeded 6,663 dead compared to Vietnam's casualty report of 58,156 (Gartner, 2013). These numbers are a direct result of better equipment, training, and the advancement in weapon systems that provide logistical support and direct combat capabilities. AT technology has been attributed as a constant guard against exploitation of these military systems while forward deployed in the battlespace. Furthermore, there is no guarantee that losses of aircraft and ground based assets during operations will be completely mitigated by damage. Therefore, the U.S. military must assume that the systems are compromised and allow for the AT technology to slow down or inhibit the exploitation process as it is designed to do (Huber II & Scott, 1999).

Long term exposure of assets in the battlespace has allowed countries such as Iran, China, and Russia to watch and learn how the U.S. and it's coalition partners conduct military operations. Long term exposure also showcases how the U.S. uses its military assests tactically and demonstrates countermeasure techniques used during contigency operations. Moreover, loss

of aircraft and ground based systems through sustained warfighting has provided many of the countries avenues in which to aquire the military asset or whole parts of the asset in order to exploit the information contained. There are many examples of this happening and clearly solidifies the need for AT integrated technology.

The purpose of this research was to examine existing security practices towards protecting military readiness from exploitation. How has the lack of security measures in past occurrences put technology at risk for compromise? What are the impacts of adapting AT technology into the acquisition life cycle? What technological advancements are utilized conjunctively to add AT protection against exploitation and reverse engineering? Which policy and procedural aspects effect the AT program's utilization throughout the Department of Defense?

Anti-Tamper (AT) technology encompasses the "systems engineering activities intended to prevent and/or delay exploitation of critical technologies in U.S. weapon systems" (Huber II & Scott, 1999, p. 356). If properly utilized, AT will increase the life span of critical technologies by increasing the capability to deter reverse-engineering by friendly and adversarial forces who advantageously want to develop countermeasures and tactics against a crucial capability. Because the advantages of exploiting these crucial capabilities empower countries and weaken the U.S., AT has been a key component of the critical systems life cycle. By introducing the AT model early in the "systems acquisition, including research, design, development, implementation, and testing" the U.S. can safely extend the effective operational life of a system, and its tactical capabilities that are formed by military operators (DoD Anti-tamper, 2013, para.1).

The Anti-Tamper/Software Protection Initiative Technology Office (AT/SPI) located at the Air Force Research Laboratory, Wright Patterson Air Force Base, Ohio, was originally established in 2000 to combat exploitation, alteration, and reverse-engineering of critical program information (CPI). The AT/SPI office now reports to the Anti-Tamper Technology Executive Agent program office (SAF/AQL) which enforces the Department of Defense Instruction 5000 series due to its sensitive nature and critical capacity.

AT is not intended to completely impede adversarial attempts to transfer or alter data and hardware functionality, but designed to dissuade exploitation of critical systems by making "such efforts so time consuming, expensive, and difficult that even if the attempts were to become successful, the AT protected technology will have been updated and replaced by the next generation version" (DoD Anti-tamper, 2013, para. 3). Overall, AT has become a crucial integrated security system for our military's technological capabilities. Due to AT technology, the U.S. can expand its global reach by selling and proliferating military hardware to coalition forces.

AT technology will provide the U.S. exportation abilities of cutting edge technology and future enhancements to its coalition allies with full interoperability enabling a stronger military presence throughout the world. The U.S. can fully field military assets placing them in operational status and simultaneously train coalition forces on how to use this technology. With this type of AT emplacement, the U.S. can provide training without fear that unapproved transfer of data and alteration of technology that will cause adverse exploitation of system capabilities (ATSPI Technology Office, 2008). In the past, U.S. policy has been reluctant to allow the sale and transfer of military hardware to foreign governments due to the lack of AT technology. The

cost of possible exploitation by foreign governments was an astronomical setback that the U.S. wanted to avoid at all cost.

> The government wants to know and track exactly what they have sold and given away. Part of the AT is preventing allies from using U.S. developed military technology in unauthorized ways. Trap doors or hidden code, for example, can be inserted into U.S. technology sold overseas to prevent its use in case of a hostile regime change. U.S. officials do not want those trap doors deactivated says Tim Teitelbaum, chief executive officer of Anti-Tamper software specialist GrammaTech Inc. (Keller, 2010, para. 19)

Additional objectives of the U.S. AT program include: military "system loss on the battlefield, exposure during the global war on terrorism, contingency operations, and cooperative activities" (ATSPI Technology Office, 2008, [Brochure Section: The opportunities for exploitation of U.S. systems are increasing]).

In the 1970s, the U.S. was friendly with the Shah of Iran and sold the Iranians 80 F-14 Tomcats at an estimated $38,000 per aircraft. The U.S. also provided flight training to Iranian pilots and support crew training in conjunction with the sale. Overall, an estimated $4 billion dollars of hardware was purchased by Iran in order to upgrade their Air Force (Military Shreds F-14s, 2007). However, in the late 1970s, the Islamic Revolution occurred and ousted the Shah of Iran in favor of replacing the government with an Islamic republic under Ayatollah Khomeini, the leader of the revolution movement. This led to a hostile regime change that now had U.S. made F-14s in their possession with training and missile assets at their disposal. There was no AT technology in place to counter the usage of these assets after the regime change. To date, Iran still utilizes F-14s in their Air Force (Military Shreds F-14s, 2007).

The F-35 Joint Strike Fighter (JSF) program is one of the latest internationally combined initiatives between twenty-five NATO countries. In 2001, the overall combined purchase of 5,000 F-35 JSF were set to take place through 2035 and would cost an estimated $63 million for each aircraft (GlobalSecurity.org, 2013). In 2003, an additional sub-contract was ordered by the DoD to create and integrate AT technologies and countermeasures adding an additional $603 million to the cost (Sweetman, 2004). However, due to technological integration and AT problems, cost increases and time delays, F-35 aircraft orders are being reduced by the international community. Due to the decrease in orders, the new estimated cost is over one billion dollars or $180 million for each aircraft (GlobalSecurity.org, 2013).

Anti-Tamper Usage Impacts Throughout History

Advancements in digital integration, hardware technology and the increase in its usage throughout everyday life have created vulnerabilities for governments and its citizens. The integration of AT technology has become a necessary standard for the protection against these vulnerabilities which can be costly and detrimental. The lack of such a standard has uncovered many instances of compromised systems over the last decade that has cost the U.S. and allies both research and development expenditures, and capabilities. The following incidents will demonstrate several adverse impacts of exploited and compromised technology due to the lack of AT countermeasures.

Enigma/World War I-II

As a direct result from World War I, signals intelligence (SIGINT) became a leading factor for intercepting and exploiting Germany's communications on the battlefield. This advantage compromised Germany's ability to successfully win World War I. Leading up to World War II, Germany's armed forces improved its compromised communications system and

looked to the private sector for newly developed technology. Germany's military acquisitions department became interested in Dr. Arthur Scherbius, who created a coded signaling device in hopes of providing secure communications for commercial businesses (Lycett, 2011).

Dr. Scherbius called his device the 'Enigma' machine, which was capable of sending, receiving, and transcribing coded messages (Lycett, 2011). In 1926, with the help of Dr. Scherbius, "the German navy was producing its own version, followed in 1928 by the army and in 1933 by the air force" (Lycett, 2011, para. 6). With the 'Enigma' machine proliferated throughout the armed forces, the German military was poised for a fluid and deceptive communications capability that created an unparalleled advantage over Allied forces.

This coded communications technology began its life cycle as a very basic system in the style of a type writer (see Figure 1). It used a combination of rotors and notched wheels with the alphabet text in order to encrypt messages sent. The system required the operator to adjust the rotors and the notched wheels in a specific sequence before producing the message. The receiver would have to know the exact sequence in order to decrypt the message, thus allowing secure communications to maintain an undecipherable capability. Throughout the war, German intelligence would produce monthly code books and send one to every military asset with an 'Enigma' machine. This would maintain the encryption cycle used by the German military (Lycett, 2011).

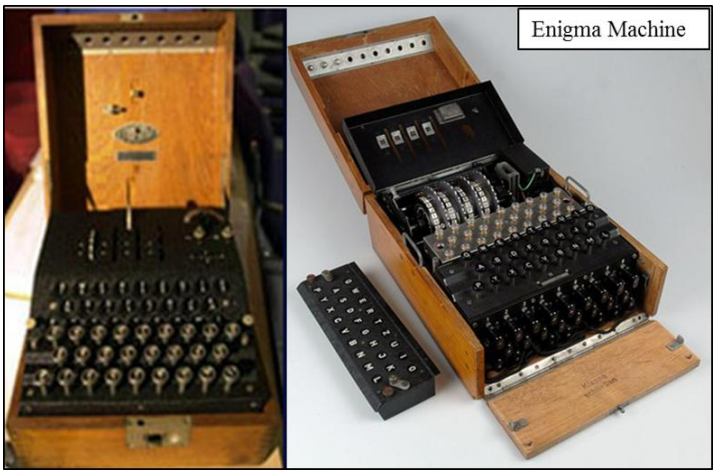


Figure 1. Germany's Enigma machine. Source, (Lycett, 2011, Enigma, 2013)

Throughout the war, Allied forces spent a plethora of resources on cracking the 'Enigma' code in order to gather strategic intelligence on enemy strength and disposition. Germany, feeling confident that the code could not be cracked, began using the code for all its communications. Because of this, the Allied forces were able to extrapolate patterns which led to the compromise of the code. In response, Germany upgraded the 'Enigma' machine with additional notched wheels and electronic circuits. These alterations provided additional cypher strings and added mathematical equations. Germany's Anti-Tamper measures once again secured the coded communications for all of its military assets. For twenty three years, Germany's 'Enigma' code machine went through a lengthened life cycle which was extended due to Anti-Tamper measures. Upgrades and modifications to the equipment assisted in the revitalization of the system while processes and procedures were in place during its employment to dissuade asset capture (Lycett, 2011).

Missile Technology

The 'Aim-9B Sidewinder' was the most advanced infrared heat-seeking missile of its time. The development began in 1946 by the U.S. Navy in order to intercept bombers and fighter aircraft through air to air engagements. The missile utilized a seeker head that contained a free

running gyroscope that spins at high speed inside a glass dome (Kopp, 1994). This technology allowed the gimbal seeker head or eyeball to maneuver angle off-boresight which allows the eyeball to look outside its peripheral view and detect radiation and heat signatures in the micron band, lock onto those signatures, and adjust its flight path to intercept (Kopp, 1994).

In the mid- 1950s, the U.S. Air Force and NATO allies adopted the AIM-9B Missile as the standard armament load for all fighter aircraft due to its reliability and lethality. The AIM-9B "drew first blood over North Vietnam… and no less than 28 Soviet MiGs were shot down" throughout the war utilizing this technology (Kopp, 1994, para. 11, 12).

The idea of AT technology had not manifested itself at this time. The standard practice was to keep positive control of the missiles and ensure that only authorized personnel had access to the asset. This type of standoff security was most prevalent and widely used until the late 1990s. Additionally, if an aircraft was shot down or missile fired during an engagement the likelihood that the missile would have been in one piece was very low and therefore un-exploitable.

On September 24, 1958 a Taiwanese F-86 Sabre aircraft engaged a MiG 17 over the skies of Vietnam. The Sabre fired an AIM-9B, hit the MiG 17 without exploding and was then lodged in the side of the fuselage. The MiG 17 pilot successfully returned to base where the missile was quickly sent back to the Soviet Union for study (GlobalSecurity.org, 2013).

The Soviets soon discovered its simplistic design made for straight forward manufacturing and mass production (see Figure 2). The Soviets also learned that their designs were too complex to maintain when fielded. Maintenance and environmental factors wreaked havoc on the successful deployment of their assets. Gennadiy Sokolovskiy, chief engineer at the Vympel team who first exploited the missile, said that "the Sidewinder missile was to us a

university offering a course in missile construction technology which has upgraded our engineering education and updated our approach to production of future missiles" (GlobalSecurity.org, 2013, para. 1).

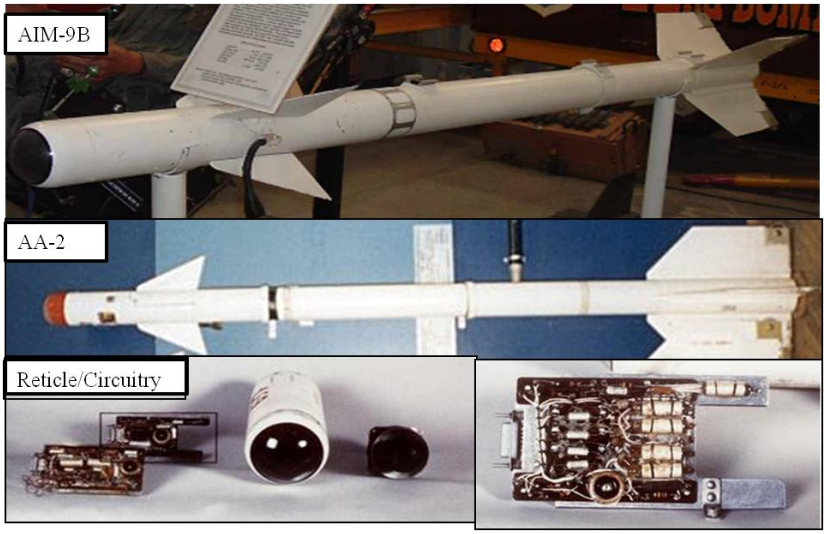


Figure 2. AIM-9 Sidewinder/AA-2 Atoll missile technology. Source, (AA-2 Atoll, 1999, Ratheon AIM-9 Sidewinder, 2013)

Following the exploitation and reverse engineering of the AIM-9 Sidewinder, the Soviets were finally able to comprehend its capabilities and the tactics used to employ it. Not only did the Soviets create their own modified version called the K-13 or AA-2 Atoll, but also created tactics for their pilots on how to employ the missile as well as defeat the U.S. AIM-9. Additionally, the Soviets produced flare capabilities as a countermeasure to the infrared missile category, which they employed on the MiG 21. The Soviets modified the body type and increasing the sensitivity of the seeker by using a cooled homing head. This allowed for higher altitude employment and an increased sensitivity to heat and radiation (GlobalSecurity.org, 2013). As the Soviets established arms dealing, this technology was sold to China and other countries decreasing the life cycle of the AIM-9B exponentially.

Intelligence Gathering Technology

On April 1, 2001 a Chinese F-8 Finback, which is an indigenously Chinese produced copy of the MiG 21, collided with a U.S. Navy EP-3 reconnaissance aircraft over the South China Sea (see Figure 3). The collision resulted in the F-8 being destroyed along with killing the pilot and crippling the U.S. EP-3, which ultimately resulted in its forced landing on China's Hainan Island (Chu & Richter, 2001).

The EP-3 is an electronic intelligence (ELINT) aircraft, it's designed to extend the long range capabilities of emissions collection and act as eyes and ears for the U.S. Navy fleet. It has the capability to intercept phone calls, fax data, email traffic, radar emissions and other sensitive data (Chu & Richter, 2001). With this capability, technology, and collected information located on the crippled EP-3, Lt. Shane Osborn, gave the order to use whatever means necessary to destroy all of the sensitive data and technology en-route. With China's Hainan Island just 70 miles away, the flight crew began smashing computers, hard drives, and monitors with hammers. One of the aircrew members later reported that he poured coffee inside the computers and all over the smashed hard drives in order to try and increase the likelihood of damage (Keller, 2010).

Figure 3. EP-3/F-8 Collision/Exploitation. Source, (Harris, 2001, NYC Aviation Staff, 2013)

Once landed, the Chinese government held the crew for ten days and impounded the plane for several months while the intelligence division stripped the plane apart, dismantling every component and examining the contents. John Pike of GlobalSecurity stated, "this airplane is basically just stuffed with electronics. Short of blowing up the airplane, there's unavoidably a limit as to what they could destroy" (Mtuck, 2001, para. 2). DoD officials believed that the Chinese government was able to ascertain and exploit data onboard the EP-3. In doing so, it was determined that the Chinese Government obtained very valuable intelligence on how the data was collected, who was being collected on, and why the data was being collected. In July, 2001, the Chinese disassembled the aircraft and shipped the plane back to the U.S. in pieces.

Within months of the EP-3 collision, the Department of Defense issued AT memos which ultimately led to the DoD Instruction 5000 series and transformed the way the U.S. military thought about AT proofing integration technology. (Keller, 2010)

Cyber Weapon

Between 2009 and 2010, a cyber-weapon named 'Stuxnet' was deployed against Iran as the first known major attack using cyberspace as the delivery method. The Natanz nuclear facility outside of Tehran was its designated target. Ralph Langner, one of the world's leading experts in cyber security, identifies that Stuxnet was designed to tamper with industrial systems built by the German company Siemens (Gross, 2011). By focusing on the S7-417 and S7-315 controllers, Stuxnet could override the supervisory control and data acquisition (SCADA) protocols, self-propagate, and send false positive readings to the main interface (Gross, 2011). After researching the attack, Ralph Langner and Microsoft assessed that there were several stages to plan, prepare for, and execute the attack. The code designs and creation consumed more than 10,000 man days to accomplish (Last, 2010). To put this in perspective, a team of thirty to fifty programmers would have to work nearly two years to accomplish the workload of researching the target, writing the code, and exploiting Microsoft's 'Zero Day' vulnerabilities. Stuxnet required not just time, but enormous technical sophistication and sizable financial resources as well (Last, 2010).

During the planning phase, not only were software engineers and programmers required, but experts in nuclear engineering were utilized to assist in designing a delivery payload that could successfully navigate around the system. In 2008, the Siemens firm cooperated with the Idaho National Laboratory in an effort to "identify vulnerabilities of computer controllers that the company sells to operate industrial machinery" (Broad, Markoff, & Sanger, 2011, para. 11). This opportunity gave the U.S. a chance to "identify well hidden holes" in the SCADA systems which were exploited the following year in Iran (Broad, Markoff, & Sanger, 2011, para. 12).

Moreover, Gross went on to say that Stuxnet was designed to utilize and circumvent code through 'Zero Day' vulnerabilities, which is poorly written or corrupted computer code within a Microsoft Windows operating system (2011). According to Gross, cyber analysts describe a single 'Zero Day' vulnerability to be extremely uncommon (2011). Stuxnet was able to utilize four of these vulnerabilities which had never been observed previously.

Stuxnet is the best known example to date of a tactical cyber weapon. After studying its behavior, it has been determined that it would only propagate itself three times, limiting its exposure to a select habitat. As of September 2010, Symantec has tracked 100,000 infected machines, 60,000 of which are located in Iran (Shakarian, 2011). Stuxnet has been traced through its coding logs and "it appears that Iran was the epicenter of the attacks", and that Stuxnet is set to self-terminate in June 2012 (Shakarian, 2011, p. 4).

Additionally, the code was only designed to attack the SCADA systems only. When the malware escaped the Natanz facility, most likely through removable media, it self-propagated throughout the Internet and became largely undetected and mostly benign to most Internet end users. However, new pieces of malware with very similar code structures started to manifest through the whole of the Internet.

Recently, malware has been discovered throughout the Internet that manifests origins of original 'Stuxnet' code. The malware 'Flame' is an "extensive data mining computer virus that has been designed to steal information from computers across the Middle East… and the 'Duqu' virus is a reconnaissance tool" that is designed to steal information from industrial systems (Perlroth, 2012, para. 1,4).

Cyber Espionage

Due to the sheer volume of classified information stolen through cyber avenues, cyber espionage has become an increasingly successful tactic used by countries who are trying to gather sensitive data. An October 2011 report to Congress on foreign economic collection and industrial espionage states: "it is part of China and Russia's national policy to identify and steal sensitive technology, which they need for their development" (Goins & Winn, 2012, para. 8). While AT technology does not play a direct role in counter cyber espionage, it does face potential exploitation when the AT technology is misappropriated along with the schematics of targeted systems during the poaching of information.

A high profile example of cyber espionage was the compromised schematic of the U.S. military's F-22 Raptor with the production of the Chinese J-20 (see Figure 4). Many key components of the aircraft were compromised along with the AT technology when the schematics were stolen which constitute a major compromise for future aircraft generations which would have used the same employed AT technology. The Chinese People's Liberation Army consists of a cyber-warfare militia that employs civilians and military personnel who have been trained and employed in high tech areas throughout China's communications and network industries. These personnel are employed to conduct hacking operations in order to gather intelligence on U.S. strategies, weapon systems, and plethora of other sensitive classified information.

Figure 4. F-22/J-20 5th Generation fighter jets. Source, (Aircraft Lovers Group, 2011, Clayton, 2012)

The J-20 has a similar delta style swept wing structure with canted horizontal stabilizers. The J-20 also has dual intakes and engines with an enclosed weapons bay for guided munitions. However, the Chinese upgraded their model after reverse engineering the baseline F-22 and added forward canards for better maneuverability at lower speeds. The Chinese also increased the size of the overall aircraft in order to add additional fuel stores, increasing the maximum range to an assessed 2,113 miles compared to the F-22's maximum range of 1,850 miles (Military Factory, 2012, F-22 Raptor Fact Sheet, 2012). These modifications effectively change the aircrafts mission from a tactical fighter to a long range interceptor and target penetrator.

With cyber-attacks increasing, defense contractors like Lockheed Martin who produces the F-22 Raptor are becoming targets in cyber espionage. The October 2011 Congressional report on foreign economic collection and industrial espionage suggests that over one trillion dollars of intellectual property, directly and indirectly has been stolen regarding the new fifth generation combat fighter aircraft (Goins & Winn, 2012). In doing so, China has been able to bypass a majority of the research and development stages saving millions of dollars and going straight to manufacturing, thus decreasing costs and final employment times.

These types of attacks provide a complicated symbiotic relationship between the U.S. Government and defense contractors. Employing private contracting companies to research, develop, and produce weapon systems, the U.S. Government can decrease costs and yet maintain a superior technological edge on the global stage. The DoD provides networks that are designed as a maze to dissuade unauthorized intrusion. They act as a barrier limiting uninhibited navigation, decelerating the exploitation and alteration of technology employed by the U.S.. These networks provide an avenue for defense contractors and military personnel to communicate and store data in a secure environment while collaborating on weapon systems development.

However, when acts of cyber espionage occur, not only do the schematics become compromised but also the integrated AT technology and all the countermeasures that are in place to protect the system. Networks, firewalls, and DoD security authentication systems are just some of the compromised countermeasures (Clayton, 2012). "Access to these designs gives China immediate operational edge that could be exploited in a conflict…accelerate the acquisition of military technology, saving billion in development costs… and benefit the Chinese government's defense industry" (Nakashima, 2013).

Anti-Tamper Policy and Documentation

The loss of military technology due to exploitation for countermeasures, reverse-engineering, and indigenously produced copies has led to the creation of several DoD initiatives (see Figure 5). The first initiative was the release of the AT policy in 1999, followed by the selection of the U.S. Air Force as the new designated AT executive agent in 2001. The first AT program tasking was to define the assessment process and begin evaluating new military equipment and technology through the acquisitions life cycle to identify which military hardware

was “subject to military capture, or loss through logistics failure or poor foreign military sales policy” (Kenny, 2009, para. 5).

Additionally, the new AT requirements and guidelines push for defense contractors and weapons system designers to identify critical program information (CPI) that will be a necessary part of the system’s functions and provide an AT plan to protect the mechanisms integrated throughout the system. By enforcing these guidelines, the DoD can incorporate AT technology during the system’s engineering designs at the principle research and development level, thus allowing for complete or symbiotic integration throughout the system’s life cycle.

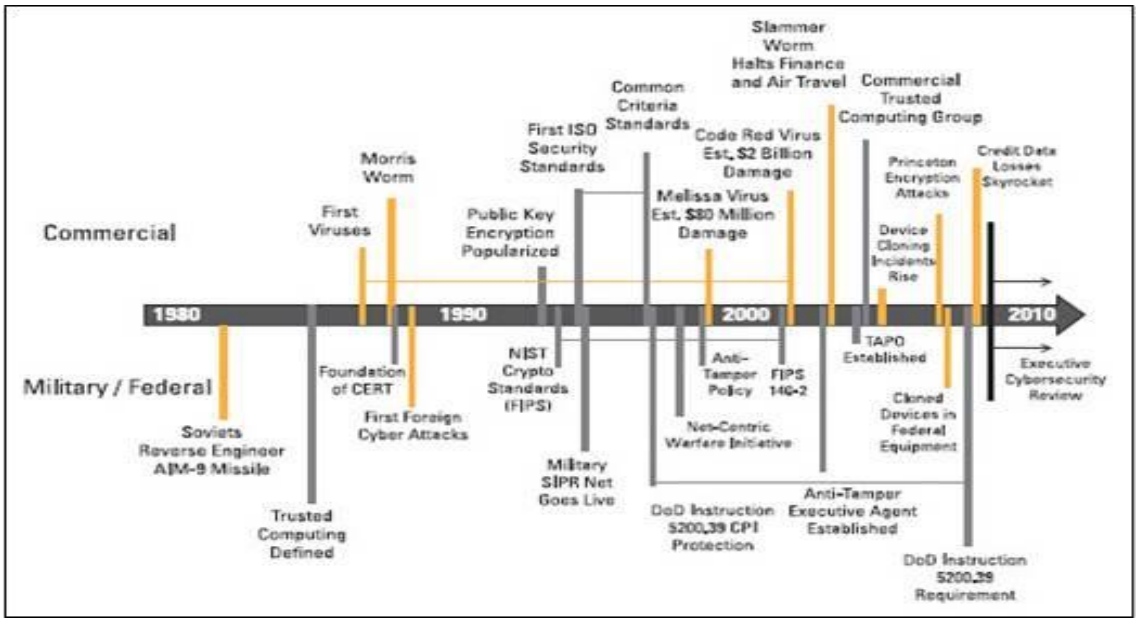


Figure 5. Historical events leading to Anti-Tamper policies. Source, (Kenny, 2009)

DoD 5200.39: CPI Protection Within the DoD/ DoD 5200.1-M Acquisition Systems Program Protection Plan

The 5200.39 instruction established policy and directives relating to the identification of and protection of CPI. These instructions are implemented by the acquisition community for the purpose of identifying and selecting critical technologies created and utilized in weapon systems by the U.S. This instruction is to be used in conjunction with DoD 5200.1-M in order to preserve

"system performance, materials, hardware, software, algorithms, design, production methods, maintenance and logistical support, and any other facets as determined by the competent acquisitions authority" (The Under Secretary of Defense, 2000, para. 2). The instruction also protects the asset by hardening the system through "intelligence, security measures, systems engineering, and defensive countermeasures… in order to mitigate risk, confidentiality, and integrity that would result in the impairment of the war fighter's capability and the DoD's technological superiority" (Department of Defense, 2008, p. 2).

There are many AT references and documentation that provide instructions and guidance for the different facets of the AT program. The documentation is utilized by DoD programs and employees as well as defense contractors. Depending on the organization and the supported mission, these references can be used single handedly or in conjunction with each other. (see Appendix A).

Utilized separately or in conjunction, these references will assist Program Managers and design personnel to evaluate the sensitivity of the technologies that are incorporated within the system (see Appendix B). During the system evaluation process, Program Managers and design personnel will address the feasibility of the system's capabilities and compare the cost of adding and integrating AT technology. This process will indicate if an AT requirement is cost effective or ineffective depending on the level of capability and the level of AT integration and protection (The Under Secretary of Defense, 2000). The ultimate goal for the Program Manager is to validate the necessary level of protection that AT gives each system while ensuring that potential risks are mitigated in a cost effective manner.

Anti-Tamper Life Cycle

The objective of the life cycle model sustains the military system through multiple phases of operation (see Appendix C). From cradle to grave, the system by design will incorporate many levels of software, hardware, configuration modes, tools, and integrated AT technology to sustain the system for the duration of necessity. The life cycle phases include material solution analysis, technology development, engineering and manufacturing development, production and deployment, and the operations and support phase. These phases are initiated through a need-driven or event-driven requirement.

The material solution analysis phase identifies the exact requirement needed to determine the types of materials needed, technological capabilities required, and life cycle cost estimates. During this phase, commercial-off-the-shelf technology solutions are considered versus developing new indigenously produced technology in order to fulfill capability requirements in a cost effective manner (Defense Acquisition University, 2010).

The technology development phase provides multiple competing teams to create the technology through hardware and software means as well as providing preliminary designs and prototypes. These teams produce full functioning systems to demonstrate the integrated technology and its capabilities. These teams usually consist of different defense contracting companies who will produce proprietary hardware and software through inclusive manufacturing and provide initial cost estimates (Defense Acquisition University, 2010).

The engineering and manufacturing development phase will determine the awarded contract recipient. The recipient will develop a full systems integration plan along with an affordable manufacturing process. In conjunction with the DoD, the defense contractor will

coordinate on how "operational supportability, reduced logistics footprint, human systems integration… interoperability, safety, utility, upgradability, and the protection of critical program information" means are identified and mitigated (Defense Acquisition University, 2010, [Graph Illustration section: Engineering & Manufacturing Development Phase])

The production and deployment phase begins with a complete, operational system that is field tested by the military. The package includes: supporting material, parts, manuals, system subject matter experts and trained military personnel who will utilize the system in an operational environment setting. The system will be utilized against other military assets during training exercises and everyday mission needs to verify the durability and desired capability of the system. This process will occur during a specified time frame as determined by DoD requirements. Initial production of this system will be limited pending the requirement of modifications to increase the durability, capability, or future modifications. This phase is also the most time consuming and costly due to testing and developing of the system (Defense Acquisition University, 2010).

Lastly, the operations and support phase sustains the system through the end of its life cycle. This phase continues with the manufacturing of the system and overlaps the production and deployment phase with the final fielded product. The manufacturing of hardware replacement parts continues in order to support the main system's functionality. This phase also supports the incremental evolutionary variants. System upgrades and variations will increase the asset protection and survivability throughout the system's life cycle.

Anti-Tamper Planning

Anti-Tamper technology planning begins with the material solution analysis phase. During this phase, AT proofing needs are assessed parallel to the systems technologies and

capabilities. Cost analysis for integrating the AT technologies are evaluated. One of the challenges of this phase is to "blend AT capabilities with commercial off-the-shelf hardware and software" that will be utilized and integrated throughout the system (Keller, 2010, para. 40). The potential for counterfeit parts will adversely negate the added AT technology countermeasures. "Protecting against counterfeit parts can be particularly important in AT because these parts can contain hidden software or access points to enable an adversary to compromise them at critical times" (Keller, 2010, para. 42). Once the initial AT plan has been authorized and the system's program initiation phase is complete, the implementation and evaluation stage begins with the technology development phase.

Anti-Tamper Implementation

Dependability, trustworthiness, and survivability are all integral components of the AT technology integration and implementation level. As the system is being built around the needs of the customer, AT technology has to be created, modified, and integrated within the software and hardware components. During the engineering design and development phase, AT integration can be incorporated into the core systems with more success at the time of the build rather than attempting to integrate the AT technology afterwards proving costly, more complicated, and less effective than otherwise noted. This multi-layered approach allows the engineers and designers to outfit the system with minimum to maximum AT countermeasures as needed by the system and the environment the system will be deployed to. In this phase, the AT technology cost ratios are also evaluated in direct correlation to the systems capabilities. The cost analysis will determine the level of protection with the cost of system loss or exploitation. Therefore, the level of AT integration can be determined and implemented as the system prototype is being developed and fielded.

Another aspect of the AT implementation is the determination of objectives that AT will accomplish to protect the intended system. The designers must decide if the AT countermeasures will deter, prevent, detect, or respond to an attack or if a collection of these measures will be implemented (Yurack, 2006). In order to identify the type of countermeasures, the designers must develop an exploitation estimate without the AT and then add viable AT measures until the desired effects are achieved. Once desired results are achieved, the final AT plan is implemented into the systems components (see Appendix D).

The verification and validation process (V&V) begins once the AT technology has been integrated and implemented (see Figure 6). The V&V testing process will ensure that the AT countermeasures work as expected in the environment the system is designed to be employed. The testing process will provide opportunities to change or upgrade the AT technology before the final product is fielded in an operational environment through consistently testing each aspect of the AT countermeasures (Yurack, 2006).

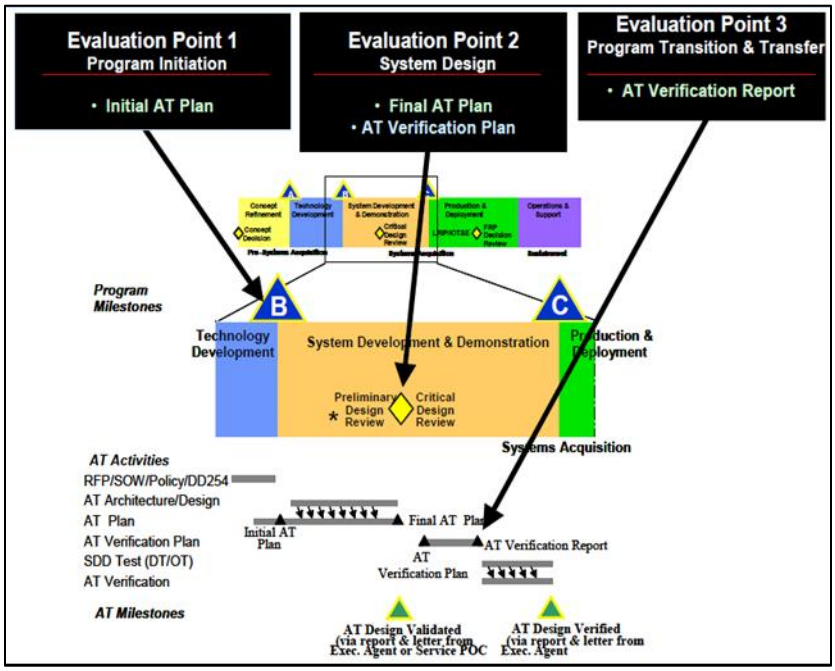


Figure 6. Validate and Verify process. Source, (Yurack, 2006).

Anti-Tamper Support Structure

The AT support structure starts at the DoD AT Executive Agent Air Force (SAF/AQL), which provides policies and documentation on how AT technology will be implemented into current and future systems (see Figure 7). The field agent for the DoD AT Executive Agent Air Force (AT-SPI Office) provides guidance for software protection and the integration of that software within hardware systems. The service leads are the branches of military that oversee the systems being created on their behalf. The field agents are the program offices onsite that test the system and oversee the life cycle process of the system from cradle to grave (Yurack, 2006).

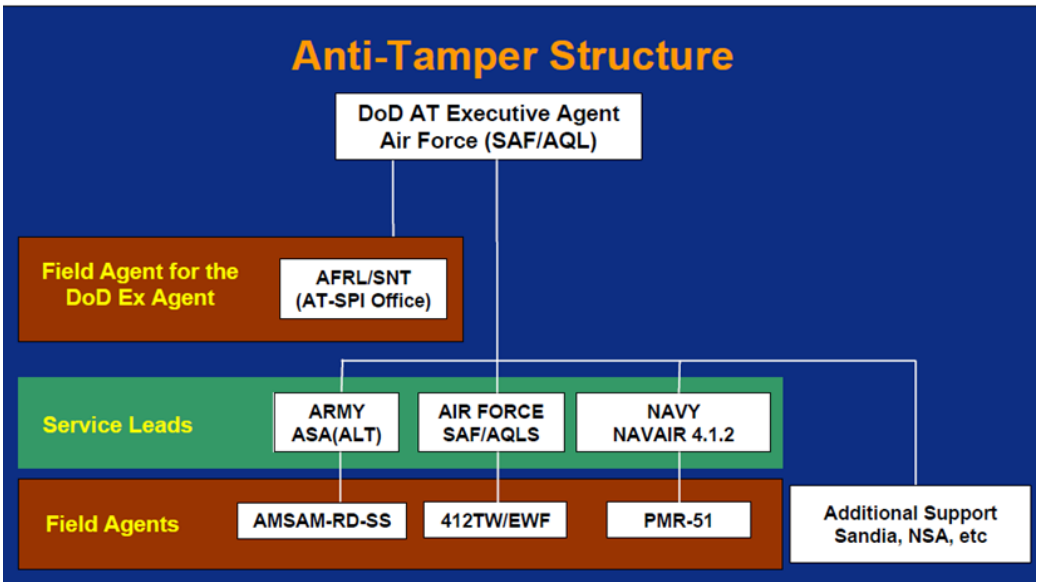


Figure 7. Anti-Tamper support structure. Source, (Yurack, 2006).

Defense Acquisition: Anti-Tamper Implementation Review Report

Between February 2003 and August 2004, the General Accountability Office completed an audit on behalf of the U.S. Senate. The audit reviewed the DoD's implementation of the AT policies. The audit revealed several issues with the AT program and several "recommendations on how to improve oversight and assist program officers in implementing AT protection on weapon systems" (U.S. Government Accountability Office, 2004, p.1).

The encountered difficulties found in the audit related to competently and accurately classifying critical technology. The baseline for determining critical technology was not present, therefore creating an atmosphere for subjective reasoning. This atmosphere obscured the selection process by reaching different conclusions depending on the point of contact. Moreover, the various organizations who participated in the AT selection process were isolated against cross data contamination and therefore did not have all the information required to make a decision (U.S. Government Accountability Office, 2004).

Another significant finding revealed that Program Managers did not have enough experience or resources available to make a proper determination on critical technologies. Additionally, program personnel saw AT technology as an additional requirement that increased costs and constrained scheduled time tables of the overall project and therefore were more likely to bypass the AT requirement by not classifying the technology as critical (U.S. Government Accountability Office, 2004).

The audit also revealed that the programs were working with budget constraints and were waiting on separate funding sources to incorporate AT technology. By following this method, AT technology was not being incorporated in the early build stages and therefore additional costs were added to the program to incorporate the AT technology at a later date. In relationship to this problem, the audit revealed that many AT techniques are not generic and are intrinsically time consuming and costly to create. AT technology creation can take longer to create than the actual system, which can delay the entire program's scheduled objectives. There are also weapon systems that cannot easily incorporate AT technology and therefore must accept a lesser security system in order to field the system and make it work correctly (U.S. Government Accountability Office, 2004).

The U.S. government Accountability Office made five recommendations in order to correct the DoD's implementation of the AT policies and procedures.

Recommendation 1: To ensure consistent identification of critical technologies throughout the Department of Defense, the Secretary of Defense should direct the Under Secretary for Acquisition, Technology, and Logistics, in coordination with the Executive Agent and focal points throughout the Services and Agencies, to continue developing a more comprehensive, standardized, and consistent critical technology identification process, and incorporate that process into Anti-Tamper policy and monitor subsequent implementation (U.S. Government Accountability Office, 2004, p. 18).

Recommendation 2: To better support Program Managers in the identification of critical technologies, the Secretary of Defense should direct the Under Secretary for Acquisition, Technology and Logistics, in coordination with the Executive Agent and its focal points, to (1) identify available Anti-Tamper technical resources and (2) issue updated policy identifying roles and responsibilities of the technical support organizations, and (3) work with training organizations to ensure training includes practical information on how to identify and protect critical technologies (U.S. Government Accountability Office, 2004, p. 19).

Recommendation 3: To minimize impact to program cost and schedule objectives, the Secretary of Defense should direct the Under Secretary for Acquisition, Technology and Logistics to work with Program Managers to ensure that the cost and techniques needed to implement Anti-Tamper protection are identified early in the system's life cycle and to reflect that practice in guidance and decisions (U.S. Government Accountability Office, 2004, p. 20).

Recommendation 4: To maximize the return of investment on DoD's Anti-Tamper initiative, the Secretary of Defense should direct the Executive Agent to assess the value of developing generic Anti-Tamper techniques and to evaluate the effectiveness of these techniques and tools in assisting Program Managers to identify and apply them on individual programs (U.S. Government Accountability Office, 2004, p. 20).

Recommendation 5: To ensure successful implementation of the Anti-Tamper policy, the Secretary of Defense should direct the Under Secretary for Acquisition, Technology and Logistics to develop a business case that determines whether the current organizational structure and resources are adequate to implement Anti-Tamper protection, and if not, what other actions are needed to mitigate the risk of compromise of critical technologies (U.S. Government Accountability Office, 2004, p. 21).

These recommendations were issued to assist in implementing a strategy to ensure success. AT technology can compete with costs and scheduled time objectives, however, AT protection is key to the survivability of a weapon system and must be integrated early and throughout the systems 'Life Cycle' in order to give a technological advantage and be effective.

Anti-Tamper Technology

Anti-Tamper is best used when several AT techniques are used in conjunction. With mutual support, the countermeasures can act as a layered protectant. No one technique can be impervious to exploitive measures. By using multiple protective technologies, certain AT methods can compensate for the shortfall of other AT methods and vice versa (Atallah, Bryant, & Stytz, 2004). Utilizing this mode of thinking, AT designers can capitalize on customizing the AT countermeasures to outfit the system for the environment in which it will operate.

Anti-Tamper protection includes several methods in order to protect the military system and the AT technology from exploitation. Tamper event monitoring provides trigger mechanisms that monitor the critical technology as well as the program information stored. This event monitoring will covertly monitor any actions and categorize the events upon detection of tamper. The monitoring system will then apply the appropriate countermeasure without any indication to the adversary that the system is being monitored (Department of the Navy, 2013).

A second protection method targets software and hardware destruction. This technology focuses on the digital and physical protection layers in place. This protection provides an avenue for the AT technology to effectively destroy key components without indicating the executed destruct mechanism employed (Department of the Navy, 2013).

Lastly, the obfuscation of AT measures employs perfidious esoteric methods in order to eliminate and render ineffective reverse engineering by adversarial methods. All three of these method types can be found in varying degrees throughout the AT program. Methods such as: software watermarking and fingerprinting, encryption wrappers, hardware based protections, and code obfuscation are just a few of how the AT program can be integrated into protected systems (Atallah, Bryant, & Stytz, 2004).

Software Watermarking and Fingerprinting

Software watermarking is a technique that infuses the software with unique identifiers that dissuade adversaries from removing the information without damaging the software. Software fingerprinting identifies and traces the illegal usage or dissemination of data by someone who exploited the software. “Watermarks may be used for proof of software authorship or ownership, fingerprinting for identifying the source of illegal information… proof of authenticity, and tamper-resistant copyright protection” (Atallah, Bryant, & Stytz, 2004, p. 15).

In conjunction, these two AT methods will secure the unauthorized usage of proprietary software that is used in association with weapon systems that can be seized by the adversary and exploited. These methods are designed to harden the system and slow down the exploitation, but not completely stop the reverse engineering process. There are several software attack methods that try to remove the software watermark and fingerprint completely, or alter it rendering the software benign thus removing the security protocols in place. If accomplished, the source code is modified, thus allowing manipulation of the software to work in such a way that its original intended purpose differs from the newly transformed version (Atallah, Bryant, & Stytz, 2004).

The AIM-9 Sidewinder's software suite that interacted with the Sabre's radar system was reverse engineered, not only through hardware means but also software recoding. Due to the lack of software watermarking, the Soviets were able to gain access to the source code and exploit the protocols (AA-2 Atoll, 1999). This allowed the Soviets to re-use the software package from the AIM-9 into their AA-2 Atoll missile and link it to the MiG's radar and avionics package. The Soviets also converted the missiles software to not only incorporate it into their legacy fighters, but also link it to newer aircraft that were being fielded and sold to other countries. (AA-2 Atoll, 1999)

Encryption Wrappers

Encryption wrappers are designed to encapsulate key software code using encryption algorithms. This type of AT security hardens a system against a "static attack, and forces the attacker to run the program in order to get an unencrypted image of it" (Atallah, Bryant, & Stytz, 2004, p. 13). However, due to encryption methods, only portions of the code enter and exit the volatile memory at a time, thus making it more difficult for an attacker to capture snapshots of the source code in an un-static environment. This type of AT security is cost effective and

provides adequate protection, thus forcing the attacker to use more cultivated assaults, which will hamper exploitation. “An encryption wrapper’s chief advantage is that it effectively hinders an attacker’s ability to statically analyze a program…which can significantly increase the amount of time needed to defeat the protection” (Atallah, Bryant, & Stytz, 2004, p. 14).

The U.S. military uses Common Access Cards (CAC) with Advanced Encryption Standard (AES) key wrap algorithms built into the chip (see Figure 8). This allows members of the armed forces, DoD civilian employees, and eligible contractors to access U.S. government facilities, controlled areas, and designated websites on the Internet using secure means of access (DoD Common Access Card, 2013).

About the size of a debit card, the CAC card is embedded with a microchip that enables a member a method to digitally sign documents, encrypt and decrypt emails, and communications through encryption and cryptographic signing. Certificates loaded onto the CAC provide the member a multifactor authenticated means of encapsulating key digital information, communicating, and accessing information via encrypted avenues (Common Access Card (CAC), 2013).

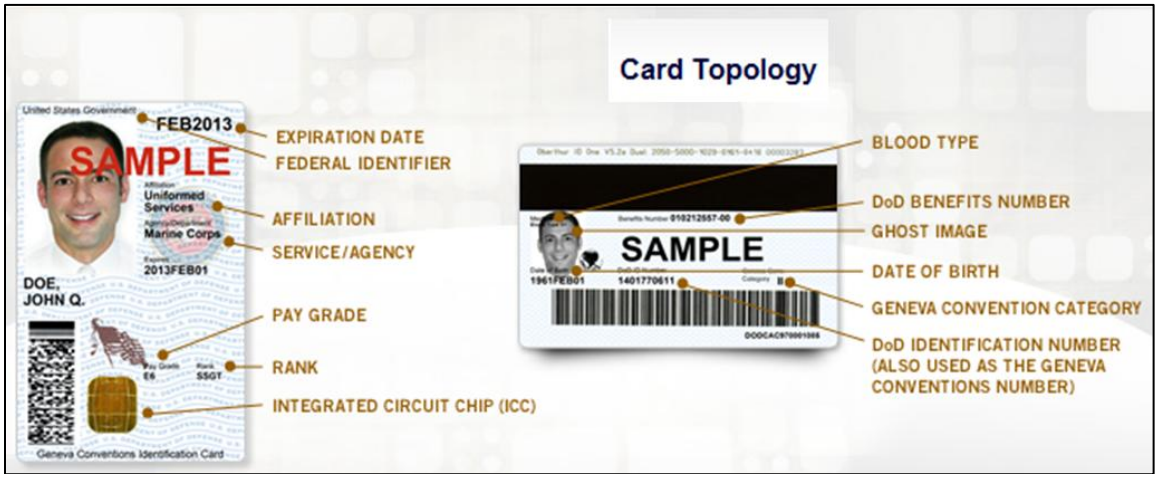


Figure 8. Common Access Card. Source, (DoD Common Access Card, 2013).

A CAC card contains a digital image of the "cardholder's face, two digital fingerprints, organizational affiliation, social security number, agency, card expiration date, and PKI certificates" (Common Access Card (CAC), 2013). The CAC card stores personalized information that relate to a member's work functions, benefits, and privileges provided by the issuing agency. Additionally, certain information stored on the CAC card can only be accessed by certain programs. For example, if dental records were stored on the CAC card, only authorized personnel with the proper application can access the dental records with permission from the CAC card owner and a PIN number (DoD Common Access Card, 2013).

Hardware-Assisted Protections

Hardware-based protections provide a different aspect of AT countermeasures. Instead of relying solely on software, the hardware itself becomes an avenue of encryption. By utilizing hardware with added inter-related subsystems that must rely on each other, weapons designers can increase the complexity of the system which will decrease the re-configurability and reverse engineering of critical hardware components. The added complexity of additional inter-related devices that communicate with each other will ensure hardening of the system against proliferation (GrammaTech, 2013).

In addition to multiple inter-related device use, hardware processing and encryption can be utilized as an additional protection. On hardware boot-up, the physical processor can complete hardware integrity checks to verify assigned hardware components. Encryption keys can be stored inside the processor to complete digital signature checks of the hardware and software. These encryption keys provide authentication between the hardware and software components, which will verify if tampering of the system has occurred. If tampering is found on

the system, then the hardware would not complete the 'post' cycle and abort the execution of loading the rest of the system on boot-up (Atallah, Bryant, & Stytz, 2004).

There are drawbacks to using hardware based protections. Maintenance issues arise when either upgrading or replacing the hardware. With all the components relying on each other, if a component breaks, then the entire system goes down. Additionally, inflexibility of modifications to post built systems increases the complexity to update the software and hardware. One major drawback to hardware protection approach "includes the expense and general fragility to accidents…either electric power surges or during fielded usage renders the processor fried and also renders the hard drive contents unusable" (Atallah, Bryant, & Stytz, 2004, p. 13).

Computer manufacturing companies utilize hardware and software assisted protections through code built in the Basic Input/Output System (BIOS) and operating systems. The BIOS restricts third party hardware installation or upgrades to limit the customization of the build. This restriction forces customers to purchase manufacturer specific hardware as replacement parts. The applied operating system also provides additional measures that verify the hardware installed on the system. Microsoft instituted a new licensing agreement with the launch of Windows Vista which limits an OEM copy of the operating system to one OEM computer. If there are any hardware changes to the original OEM hardware, the operating system will no longer work unless the OEM hardware is replaced with the exact OEM specified hardware (Microsoft, 2013).

Code Obfuscation

Code obfuscation is the process of obscuring and altering the computer code making it in-cognizable to humans, thus defusing exploitation by making the system more impenetrable. This method of AT protection increases the technical challenge of application in systems. By applying

this method to cultured software, there "is a danger of introducing subtle bugs, or not introducing sufficient protection…. and this method is too effective at protecting small samples but doesn't offer sufficient guarantees of protection for large applications" (GrammaTech, 2013, para. 1)

There are several methods of code obfuscation. Layout obfuscation modifies the physical appearance of the code by changing the variables with random strings and transforms the structured layout of the code (Atallah, Bryant, & Stytz, 2004). Data and control obfuscation changes the data structure of the code by merging or splitting the code into different sections, thus creating a chaotic representation of the data code (Atallah, Bryant, & Stytz, 2004). Preventative transformations make it problematic for de-obfuscation programs to reverse the obfuscation of data and find the original code structure, thus denying the reverse engineering process (Atallah, Bryant, & Stytz, 2004).

Oracle PL/SQL code is used to create and maintain databases. Inside the Oracle software there is a wrap utility that provides code obfuscation. This provides added security when sending the code or scripts via unsecured means to external customers in order to protect the source code. Without the wrap utility, a third party can intercept the source code, make a duplicate and modify it for personal use. Additionally, the code obfuscation feature can limit customers from modifying the source code to get around the set parameters and limitations, thus dissuading company revenue loss (Stephens, 2004).

Discussion of Findings

The purpose of this research was to examine existing security practices towards protecting military readiness from exploitation. How has the lack of security measures in past occurrences put technology at risk for compromise? What are the positive and negative impacts of adapting AT technology into the acquisition life cycle? What technological advancements are

utilized conjunctively to add AT protection against exploitation and reverse engineering? Which policy and procedural aspects effect the AT program's utilization throughout the Department of Defense?

The mission of AT technology encompasses the "systems engineering activities intended to prevent and/or delay exploitation of critical technologies in U.S. weapon systems" (Huber II & Scott, 1999, p. 356). If properly utilized, AT will increase the life span of critical technologies by increasing the capability to deter reverse-engineering by friendly and adversarial forces who advantageously want to develop countermeasures and tactics against a crucial capability.

The German 'Enigma' machine is a quintessential example of how AT measures assisted in maintaining a technological advantage over an adversary during combat operations through the life cycle duration of acquisition, manufacturing, and development phase to the deployment, sustainment, and disposal phase (Defense Acquisition University, 2010). The act of changing components and adding additional notched wheels and electronic circuits provided the AT needed to gain the technical edge (Lycett, 2011). Changing the cipher keys constantly provided the AT needed to control and maintained the security edge (Lycett, 2011). Additionally, by producing and forward deploying the Enigma machine to key locations provided AT needed to secure the infrastructure of the secure communications (Lycett, 2011). Studies show that by accomplishing consistent changes and upgrades to the actual technology, maintained security, and the fortified methods of fielding the technology, Germany was able to maintain a steady advantage throughout the war (Lycett, 2011).

However, the mindset of AT integration was not fully developed in the years following World War II and the Korean War. The U.S. valued the propagation of military hardware and

advancing technology in an expeditious manner over the actual protection of the technology. In doing so the U.S. learned a valuable lesson with the exploitation of the AIM-9 Sidewinder.

The AIM-9 Sidewinder is a prime instance where a military asset provided an invaluable technology for U.S. and allies during contingency operations. Unfortunately, due to a malfunction during its employment and lack of integrated AT technology, the missile was captured and exploited. It is evident that this missile cost the U.S. and allies not only a capability, but research and development costs, a tactical edge for the warfighter, and the new infrared missile technology that would proliferate in every aircraft and missile from then on. Developing integrated AT technology at the beginning of the AIM-9's life cycle would have provided adequate protection of the missile during the fielded deployment and would have maintained the technological advantage throughout the Vietnam conflict slowing the proliferation of missile technology to the Soviets.

The EP-3 incident is a perfect example of the lack of integrated AT technology within an intelligence gathering asset. Not only was the aircraft compromised, but all of the culminating technologies on board that made up the asset. Specialized signals and electronic gathering equipment were unprotected due to insufficient understanding of possible compromising scenarios. Evidence shows that the aircrew personnel were unprepared to properly destroy the classified equipment when they tried to pour coffee onto the hardware systems. The procedure in place for destruction of classified information was murky at best and the lack of training was apparent. However, due to this incident, the DoD began implementing policies and procedures for new technology and proper destruction methods for existing technology. This incident forced the U.S. military to start thinking about sufficient countermeasures for military assets and the

proper training of individuals to ensure the protection of those assets while in a forward deployed location accomplishing the mission.

The Stuxnet worm was a higly prized piece of code that, left out in the open, could cause major damage if captured and reverse engineered. Considering this, the creators implemented a 'self-terminate' code within Stuxnet that removed itself from every infected machine and destroyed itself in June 2012 (Shakarian, 2011). This type of built in code that forced the malware to self-terminate is a perfect example of AT technology integrated within the deliver platform. However, the 'Flame' and 'Duqu' are two new pieces of malware that were reverse engineered from the 'Stuxnet' virus. When the Stuxnet virus was deployed, pieces of the virus were exploited and eventually mutated to fit the needs of their creators. This exemplifies the reverse engineering process and advancement in capabilities through remnants of code left behind on the Internet. AT technology in this case contributed to the slowing of proliferation and alteration of the malware code. The AT technology was not totally successful in protecting against exploitation and reverse-engineering. However, this example does provide insight as to the possibility of integrating AT countermeasures into future cyber weapons. By providing an avenue to upgrade and incorporate variations of AT technology, cyber weapons can be hardened against exploitation during and after employment.

Along with malware such as the Stuxnet virus, more governments are using computer code to attack targets and gather intelligence on foreign governments. Cyber espionage has been found to facilitate the extraction of information before it can be hardened physically, thus exploiting the digital data before manifestation into physical form.

The Chinese J-20 incident demonstrates how various governments are not waiting until a weapon system is fielded with AT technology integrated into the system before capturing,

exploiting and reverse engineering it. Countries like China and Russia are now trying to capture these technologies at the beginning of their life cycle so as to bypass many of the countermeasures that are put in place along the stages of production. AT technology must be integrated on day one of the acquisition and life cycle phase of each weapon system in order to protect the weapon system from cyber espionage as well as the protection of the AT technology itself.

The above example vilifies the idea of overcoming the U.S. AT countermeasure standards that are currently in place. By attacking the infrastructure and the life cycle process, a government or third party participant can gain access to the system designs and its potential capabilities, but also the scheduled AT plan and its integrated countermeasures. If these AT technologies become compromised, evidence shows that other assets that are concurrently fielded with the same AT technology are considered unprotected and therefore easy targets for potential compromising if captured, sold, or left on the battlefield during combat operations.

The AT compromise will also slow down the life cycle process, the systems in the pipeline and future systems which are using or are scheduled to use the same type of AT countermeasures. This has the potential to be costly and time consuming for the U.S. military. By playing out this scenario, the DoD would have to create new AT technologies constantly only to have them compromised and ineffective thus rendering the entire AT program non-effective and unusable.

Regardless of the positive idea that AT policies and documentation are detailed and thorough, this study has shown that the requirements for AT protection are the least developed and least documented. It is clear that the sources for the DoD are instruction 5200.39 and the DoD 5200 series manuals (Yurack, 2006). These manuals direct DoD officials, defense

contractors, and Program Managers on the requirements of having in place a program protection plan. This plan "identifies all the CPI in a defense system and a plan to protect that information in case of a security breach or reverse engineering" (Kenny, 2009).

However, a major concern regarding the policies in place have to do with the instructions themselves and the adverse reaction they are having on the entire AT program. Not only are the instructions confusing, lacking information, and redundant at best, but there is no strict guidance and standards that force the compliance of the 5200.39, 5200 series, and the personal protection program. The instructions lack the basis to properly define what a critical technology is and force the Program Managers to define a critical technology and the requirements needed for AT integration (U.S. Government Accountability Office, 2004). By placing the Program Managers in this position, they are susceptible to incorrect categorization, pressure from outside influences who are working against cost savings and time deadlines, and insufficient security requirements that pertain to the specific system.

Additionally, much of the policy and documentation does not keep pace with newer technology. DoD instruction 5200.39 is reviewed and changed every 2-3 years. The DoD incorporated a change to the policy and updated from the July 16, 2008 edition to the December 28, 2010 edition (Department of Defense, 2008). This is the last edition that has been approved thus far. With several years in between editions, technology advancements continue to surpass DoD guidance and will provide outdated methods to incorporate AT technology.

A major concern made clear by the 2004 U.S. General Accounting Office audit involves the integration and implementation procedures throughout the life cycle process. It is apparent and disconcerting that policies and documentation regarding AT implementation are not being

followed. Either by confusion of written policy or by neglect, Program Managers and defense contractors are not following guidelines set forth by the DoD.

During the audit, there were several findings that proved implementation difficulties occurred. First, the lack of defining what a critical technology is makes it difficult for Program Managers to know what asset AT technology must be applied to. Second, additional resources were not available to assist in defining these critical technologies and therefore provided no support to Program Managers. Third, AT technology increases the complexity of the weapon system and increases the development and designing stages, thus ultimately putting the entire weapons system in danger of being cancelled due to the technical difficulties of incorporating AT technology within the system. And lastly, the idea of AT technology is seen as an additional costly feature that impacts the system's overall cost and causes time delays without any indication of increasing the capability of the system and therefore is discouraged by the weapon system designers (U.S. Government Accountability Office, 2004).

It is apparent that the idea of AT technology is considered a costly insurance without any added benefit to the system except for when an unforeseen disaster takes place. In order for the AT integration process to be successful, there needs to be a fundamental shift in mindset. All those involved in the acquisitions process should think of the AT program as part of the system and not as an afterthought to the system. The DoD must incorporate the AT requirements along with the system at the time of the contract bid. Otherwise defense companies will see the system and the AT technology as two separate entities instead of one total system.

The research shows an apparent lack of education on AT technologies and techniques available throughout the industry. Without being educated on new data and AT security practices, Program Managers could inhibit the growth of AT countermeasures in newer military

systems by deciding on less effective and substandard practices to protect assets as they move through the life cycle.

The JSF exhibits some of the issues of not integrating AT technology at the beginning of the life cycle. The study shows that in 2003, several years after the program was commissioned, a supplemental contract was awarded to Lockheed Martin to create and incorporate AT technology into the JSF. The contract cost the DoD an extra $603 million and an expected one billion dollars total to retrofit and integrate AT countermeasures into the JSF aircraft (Sweetman, 2004). Integration of AT technology into legacy systems and newer systems that have already been initiated through the life cycle process will be costly and logistically incomprehensible to the DoD, due to newly found AT requirements set forth by DoD policies and procedures.

Defense companies such as; Lockheed Martin, Boeing, SAIC, BAE systems, and Northrop Grumman all provide services through DoD contracts. Many contracts include one or more differing companies to work together to fill these contracts. Research shows that when multiple defense contractors work on military systems collectively, integration of proprietary technology manifests issues when integrating AT countermeasures.

Hardware-based countermeasures through hardware sub-systems can be cumbersome when integrating key components produced by different companies. Trying to produce AT techniques to protect those systems without being able to access the proprietary software can cause not only incompatibility between systems, but can cause unwanted AT results. During the build for the JSF, the AT technique, low observable (LO) was introduced. This feature deals with the stealth technology piece of the aircraft and shields the system from being detected by radar. This technology is proprietary to Lockheed Martin and the designs had to be adjusted in order to

accommodate different sub systems that were being built and implemented into the foreign purchased JSF aircraft (Sweetman, 2004).

The JSF program illuminates the difficulties of integrating AT technology into an aircraft that has been purchased by multiple countries in a joint effort to upgrade multiple Air Forces. The act of incorporating differing technologies from different companies from various countries has placed an excessive strain on the AT program. Each country has different security requirements that must be incorporated into the JSF. The foreign purchased or 'international' model that is being built will have a larger radar cross section and therefore be seen by radar systems easier than the U.S. version and therefore are predisposed to attack. The U.S. variant will also have a different avionics package, which will be more capable than its international counter-part. With these types of differences, AT technology must be created and applied at different levels of the aircraft in order to protect the different capabilities, but also the AT technology itself. With this international undertaking in progress, US officials are worried that an international model will be acquired by China and Russia. If this happens then the JSF could become exposed, exploited, and reverse engineered thus rendering the capabilities counter measured (Sweetman, 2004).

Research also shows that because of the numerous companies and sub-contracts being created for the JSF program, there is a high likelihood that some of those companies will terminate their contracts due to bankruptcy. When this happens, the proprietary software and hardware is no longer supported by that particular company rending the software or hardware unusable. During the lifecycle phase, AT integration can become affected by requiring the security measures to be revamped in order to integrate new technology from a different company or by gap filling the technology that will no longer be applied at all. This process becomes costly

and creates time delays which could cause the AT technology to be ineffective or not applied to that specific system before it is fielded.

There are several factors that are lacking within the DoD acquisitions program. Historically, weapon systems are fielded without the integration of AT countermeasures. Only after several major compromising incidences occurred was there a fundamental shift in mindset regarding AT technology. However, the support structure, ideology, and knowledge are lacking in order to create, integrate, and maintain the upgrade of AT technology in current systems. The program security offices involved muddies the clarification needed to maintain transparency throughout the 'Life Cycle' phases.

Overall, AT technology and its integration are key components to maintaining superior war fighting capabilities. This study manifested historical examples of when war fighting capabilities were exploited due to the lack of AT integration. The study focused on current DoD policies and industry practices that are utilized today in order to protect legacy, new, and future systems. This research was hindered by the sensitive nature of the technology being incorporated in today's military assets. All sources and citations are open source and readily available to the public. Many of the issues and technological breakthroughs are not discussed in this research due to the sensitive nature which could expose capabilities and vulnerabilities in the AT process.

Recommendations

Some recommendations are strongly advised for the DoD and defense industry in relation to the creation and integration of AT technology during the life cycle phase of military assets. While current methods of integration are adequate, there are many areas of the AT process that could be improved in order to assist in cost savings, best practices, and more secure methods.

Policies and Procedures

It is recommended that DoD policies, such as the 5000 series and any additional supporting documentation, needs to be updated annually. This will provide clear, concise, and updated guidance and provisions on new technology and procedures that have been deemed as best practices throughout the previous year. These clear provisions will assist contractors and DoD Program Managers to take logical and intelligent steps of processing administrative paperwork as well as accomplishing the creation of AT technology, its integration, and any modifications inside and outside the life cycle process.

Working Committee

It is advised that the DoD create a separate AT working committee consisting of representatives from the U.S. military and government agencies to provide subject matter experts on the weapon systems usage and recommendations of AT integration. This committee will have the authority to identify a weapon system's level of AT countermeasures if any and work closely with AT developers and Program Managers to enforce proper level AT integration.

This committee will be responsible for a complete overhaul of the AT process and remove total authority and administrative responsibilities from the Program Managers and defense contract liaisons that are managed by cost constraints and time objectives. This committee will ensure the validity of AT integration while keeping an unbiased approach to the level of required AT techniques throughout the life cycle.

Moreover, the committee will review the DoD policies annually and make recommendations for changes and improvements in order to streamline the process of AT integration. The committee members will complete an annual compliance inspection of all departments. This inspection will include all documentation, on-site visits, and a feedback report

including best practices and an area of improvement recommendations. This committee along with annual reviews and inspections will provide avenues for improvement and unbiased oversight which will decrease costs, unnecessary policies and guidelines, and an increase in best practices, thus streamlining the life cycle and AT integration process.

End User Anti-Tamper Training

It is endorsed that personnel who utilize the fielded system are provided advanced AT training, checklists, and tools to properly execute their portion of the countermeasure in order to protect the asset from exploitation if captured during a contingency operation. Not all AT technology is inclusive to protecting and sanitizing data. Personnel who utilize the system can also ensure AT protection by accomplishing key tasks to sanitize data and hardware functionality before being captured.

Customizable Anti-Tamper Technology

It is proposed to create customizable AT technology for different systems. Different variations of the same AT countermeasures can increase the unlikely compromise of separate systems being produced and fielded. This will be a cost effective practice that can utilize variation of AT technology rather than creating personalized AT countermeasures for each individual system. This practice will assist in an administrative capacity by already having the technology created and approved through the committee. This practice will speed up the AT test and development stages as well as the integration process while providing baseline commonality in software and hardware practices.

Legacy Integration Practices

It is suggested that AT technology not be incorporated into legacy systems. Legacy systems have been designed without the integration of AT countermeasures. These systems will

face potential integration problems with the introduction of added software and hardware technology. The cost of adding these protections could outweigh the benefit of the legacy system and run the risk of not extending the life of the system. Additionally, many of these legacy systems have already been sold to foreign governments who most likely have already exploited the vulnerabilities and even reverse engineered it. There is no reason to protect the asset's capabilities after the fact. However, if there is an added capability such as a missile or radar technology that is not a part of the system but utilized by the system, then AT technology should be used to protect that asset.

In the past thirteen years, great strides have been surpassed, barriers overcome, and technological advancements that have been made in AT technology. Although, the DoD and the defense industry have made great progress, AT technology and its integration are still in the infancy stages of the acquisition process. There is still much more that needs to be realized.

Future Research Recommendations

Future research in areas of AT creation and integration, as well as program management, and policies and procedural implementation needs to be streamlined and standardized. Feedback should be requested from the war fighters who utilize the weapon systems in the field to assist engineers in advancing AT technology and provide better training to those who use it. Digital espionage should be studied further in order to harden the digital infrastructure that protects the acquisitions program and the infused AT technology. Lastly, future research needs to be conducted on the statistical analysis of all historical examples of compromised weapon systems that included and excluded AT technology. Perhaps in doing so, a fundamental ideological shift will occur in the acceptance of AT integration as a standard practice and not an added burden.

The future of AT technology and integration is vital to the success and unyielding superiority of the U.S. military and Allied forces. Without AT technology, it's only a matter of time before the chink in the armor is found and exploited.

References

AA-2 Atoll. (1999, March 21). Retrieved from FAS Military Analysis Network: http://www.fas.org/man/dod-101/sys/missile/row/aa-2.htm

Military Shreds F-14s. (2007, July 03). Retrieved from Military.com: http://www.military.com/NewsContent/0,13319,140944,00.html

Aircraft Lovers Group. (2011, February 21). Retrieved from www.moddb.com: http://www.moddb.com/groups/aircraft-lovers-group/images/su-27j-20j-xxpak-fa-t-50f-22a

F-22 Raptor Fact Sheet. (2012, May 8). Retrieved from U.S. Air Force: http://www.af.mil/information/factsheets/factsheet.asp?id=199

Common Access Card (CAC). (2013, July 03). Retrieved from TechTarget: http://whatis.techtarget.com/definition/common-access-card-CAC

DoD Common Access Card. (2013, July 03). Retrieved from www.cac.mil: http://www.cac.mil/common-access-card/

Enigma. (2013, May 15). Retrieved from The National Museum Royal Navy: http://www.nmrn.org.uk/explore/curators-highlights/enigma

Ratheon AIM-9 Sidewinder. (2013, May 15). Retrieved from Marvellous Wings: http://www.marvellouswings.com/Aircraft/Missile/M-009/M-009.html

Atallah, M. J., Bryant, E. D., & Stytz, M. R. (2004, November). *A Survey of Anti-Tamper Technologies*. Retrieved from CrossTalk: The Journal of Defense Software Engineering: www.crosstalkonline.org/storage/issue-archives/2004/200411-atallah.pdf

ATSPI Technology Office. (2008, May 27). *Anti-Tamper Program Brochure*. Retrieved from http://at.dod.mil:

https://www.google.com/url?q=https://dap.dau.mil/policy/Documents/Policy/Anti-Tamper%2520Program%2520Brochure.pdf&sa=U&ei=n7VlUYWxA6_W0gHr2YDQCw&ved=0CAsQFjAC&client=internal-uds-cse&usg=AFQjCNEj1c0bxHmmsajbMsTxRuDX9GWnXg

Broad, W. J., Markoff, J., & Sanger, D. E. (2011, January 16). *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*. Retrieved from New York Times: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all

Chu, H., & Richter, P. (2001, April 2). *U.S. Spy Plane, Chinese Fighter Collide Over Sea*. Retrieved from the Los Angeles Times: http://articles.latimes.com/2001/apr/02/news/mn-45841

Clayton, M. (2012, November 14). *U.S. cybersecurity report points accusing finger at China*. Retrieved from The Christian Science Monitor: http://www.csmonitor.com/USA/Politics/2012/1114/US-cybersecurity-report-points-accusing-finger-at-China

Defense Acquisition University. (2010, June). *Integrated Life Cycle Chart*, 5.4. (D. A. University, Producer) Retrieved from Defense Acquisition University: https://ilc.dau.mil

Department of Defense. (2008, July 16). *DoD Instruction 5200.39*. Retrieved from www.dtic.mil: http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf

Department of the Navy. (2013, May 06). *Anti-Tamper Protection of Critical Systems*. Retrieved from Office of Naval Research: http://www.onr.navy.mil/en/Media-Center/Fact-Sheets/Anti-Tamper-Protection.aspx

DoD Anti-tamper. (2013, May 10). *Introduction to Anti-Tamper*. Retrieved from DoD Anti-tamper: https://www.at.dod.mil/

Gartner, S. S. (2013, April 03). *Iraq and Afghanistan through the Lens of American Military Casualties*. Retrieved from Small Wars Journal: http://smallwarsjournal.com/jrnl/art/iraq-and-afghanistan-through-the-lens-of-american-military-casualties

GlobalSecurity.org. (2013, May 11). *AA-2 ATOLL*. Retrieved from Global Security: http://www.globalsecurity.org/military/world/russia/aa-2.htm

GlobalSecurity.org. (2013, June 06). *F-35 Joint Strike Fighter (JSF) Lightning II*. Retrieved from GlobalSecurity.org: http://www.globalsecurity.org/military/systems/aircraft/f-35-int.htm

Goins, C., & Winn, P. (2012, April 25). *Chinese Hackers Stole Plans for America's New Joint Strike Fighter Plane, Says Investigations Subcommittee Chair*. Retrieved from CNSNews.com: http://cnsnews.com/news/article/chinese-hackers-stole-plans-americas-new-joint-strike-fighter-plane-says-investigations

GrammaTech. (2013, May 06). *Air Force Research Laboratory Anti-Tamper/Software Protection Initiative*. Retrieved from GrammaTech Completed Projects: http://www.grammatech.com/research/sponsors/afrl-spi/deobfuscating-tools-tamper-proof-software

Gross, M. J. (2011, April). *A Declaration of Cyber-War*. Retrieved from Vanity Fair: http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104#

Harris, R. (2001). *Spyplanes, Spyships, & Seizures: A deadly dance of dark suspicion* . Retrieved from Iwichita.com: http://home.iwichita.com/rh1/hold/av/avhist/mily/spyplane.htm

Huber II, A. F., & Scott, J. M. (1999). *The Role and Nature of Anti-Tamper Techniques in U.S. Defense Acquisition*. Retrieved from DTC Online: Information for the Defense

Community: http://oai.dtc.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier-ADB250068

Keller, J. (2010, April 26). *Anti-Tamper Technologies Seek to Keep Critical Military Systems Data in the Right Hands*. Retrieved from Military & Aerospace Electronics: http://www.militaryaerospace.com/articles/2010/04/anti-tamper-technologies-seek-to-keep-critical-military-systems-data-in-the-right-hands.html

Kenny, R. J. (2009). *Processing Security - A Dimensional Requirement*. Retrieved from GSA Global: http://www.gsaglobal.org/forum/2009/2/articles_kenny.asp

Kopp, C. (1994, April). *The Sidewinder Story: The Evolution of the Aim-9 Missile*. Retrieved from Ausairpower.net: http://www.ausairpower.net/TE-Sidewinder-94.html

Last, J. V. (2010, December 13). *How the Worm turned*. Retrieved from Weekly Standard: http://www.weeklystandard.com/articles/how-worm-turned_520704.html

Lycett, A. (2011, February 17). *Breaking Germany's Enigma Code*. Retrieved from BBC History: http://www.bbc.co.uk/history/worldwars/wwtwo/enigma_01.shtml

Microsoft. (2013, June 05). *Legal and Corporate Affairs End User License*. Retrieved from Microsoft.com: http://www.microsoft.com/en-us/legal/intellectualproperty/UseTerms/default.aspx

Military Factory. (2012, August 23). *The Ghengdu J-20 is expected to reach operation status in 2018 with the Chinese Air Force*. Retrieved from Military Factory.com: http://www.militaryfactory.com/aircraft/detail.asp?aircraft_id=860

Mtuck, D. (2001, March 31). *U.S. Spy Plane Crashes in China; Chinese Strip Plane of Sensitive Equipment*. Retrieved from History Commons:

http://www.historycommons.org/timeline.jsp?us_military_specific_cases_and_issues=us_military_tmln_spy_plane_crash_in_china&timeline=us_military_tmln

Nakashima, E. (2013, May 27). *Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies*. Retrieved from Washington Post: http://articles.washingtonpost.com/2013-05-27/world/39554997_1_u-s-missile-defenses-weapons-combat-aircraft/2

NYC Aviation Staff. (2013, May 15). *China Releases U.S. Navy Airmen*. Retrieved from NYC Aviation: http://www.nycaviation.com/2012/04/april-11th-in-aviation-history-worlds-youngest-pilot-dies-in-plane-crash-china-releases-captured-navy-airmen-following-hainan-island-incident/

Perlroth, N. (2012, May 30). *Researchers Find Clues in Malware*. Retrieved from The New York Times: http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html

Shakarian, P. (2011, April 14). *Stuxnet: Cyberwar Revolution in Military Affairs*. Retrieved from Smallwarsjournal.com: http://smallwarsjournal.com/jrnl/art/stuxnet-cyberwar-revolution-in-military-affairs

Stephens, S. (2004, June 2). *Oracle Tip: The wrap utility and code obfuscation*. Retrieved from TechRepublic: http://www.techrepublic.com/article/oracle-tip-the-wrap-utility-and-code-obfuscation/5224544

Sweetman, B. (2004, April 05). *Anti-Tamper technology for the JSF-costs $1 Billion Extra*. Retrieved from The Aviation Forum: http://forum.keypublishing.com/showthread.php?24408-anti-tamper-technology-for-the-JSF-costs-1-billion-extra

The Under Secretary of Defense. (2000, May 3). *Guidelines for Implementation of Anti-Tamper Techniques in Weapons Systems Acquisition Programs*. Retrieved from dap.dau.mil: https://dap.dau.mil/policy/Documents/Policy/Guidelines%2520for%2520Implementation%2520of%2520Anti-Tamper%2520Techniques%2520in%2520Weapon%2520Systems%2520Acquisition.docx

U.S. Government Accountability Office. (2004, March 31). *Defense Acquisitions:DOD Needs to Better Support Program Managers' Implementation of Anti-Tamper Protection*. Retrieved from GAO: U.S. Government Accountability Office: http://www.gao.gov/products/GAO-04-302

Yurack, J. (2006, October). *Anti-Tamper Overview and V&V Process*. Retrieved from DoD Anti-Tamper Executive Agency: http://www.google.com/url?sa=t&rct=j&q=DoD+anti-tamper+&source=web&cd=3&cad=rja&ved=0CEIQFjAC&url=http%3A%2F%2Fwww.dtic.mil%2Fndia%2F2006systems%2FThursday%2Fyura.pdf&ei=GRSAUa3pA-7q2wWkxoHgCA&usg=AFQjCNHrISO7dBKcg4cf3aEZg4tCPY7lLA&bvm=bv.45645796,d.b2I

Appendices

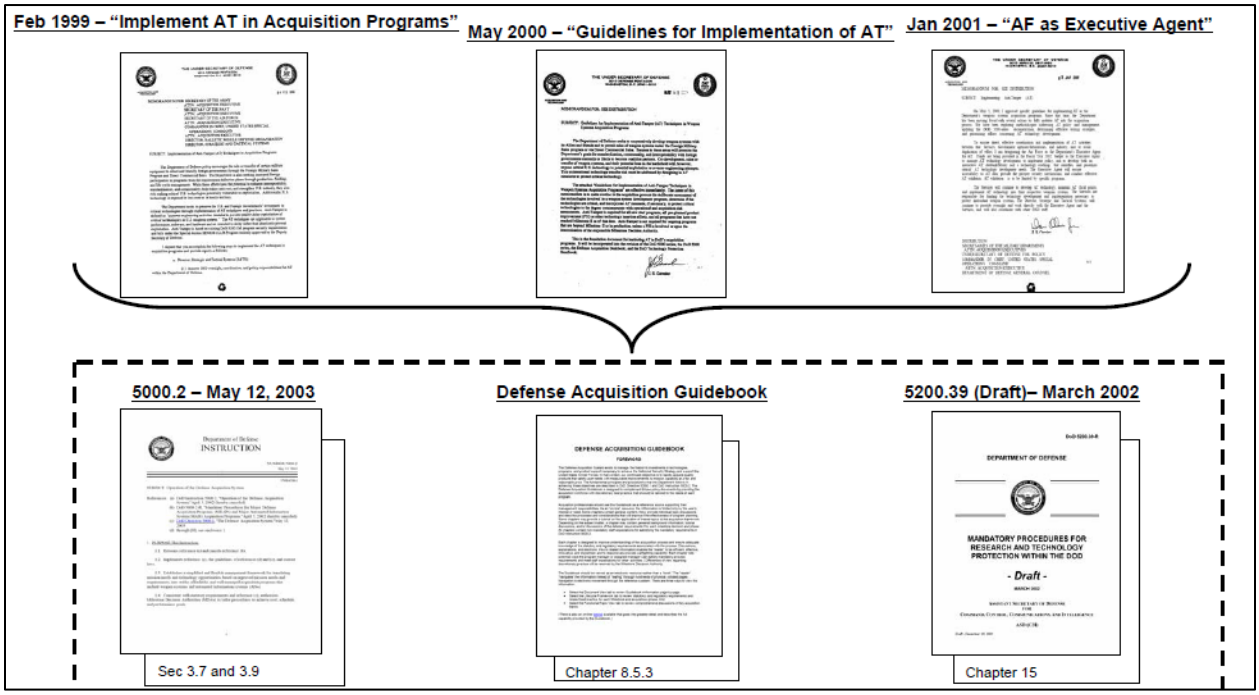
Appendix A –

Anti-Tamper References and Documentation

- USD (A&T) Memorandum, "Guidelines for Implementation of Anti-tamper Techniques in Weapon System Acquisition Programs," 1 May 2000
- DoD Instruction 5000.2 "Operation of the Defense Acquisition System," 12 May 2003
- Defense Acquisition Guidebook (www.dau.mil)
- Military Critical Technologies List (www.dtic.mil/mctl)
- USD (A&T) Memorandum, "Implementing Anti-Tamper," 5 January 2001
- Safe Array Compartment Security Classification Guide, 11 July 2005, SAF/AQL
- CJCSI 3170.01D, "Joint Capabilities Integration and Development System," 1 May 2007
- DoD Directive 5200.39, "Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection, 16 July 2008
- DoD 5200.1-M, "Acquisition Systems Program Protection Plan"

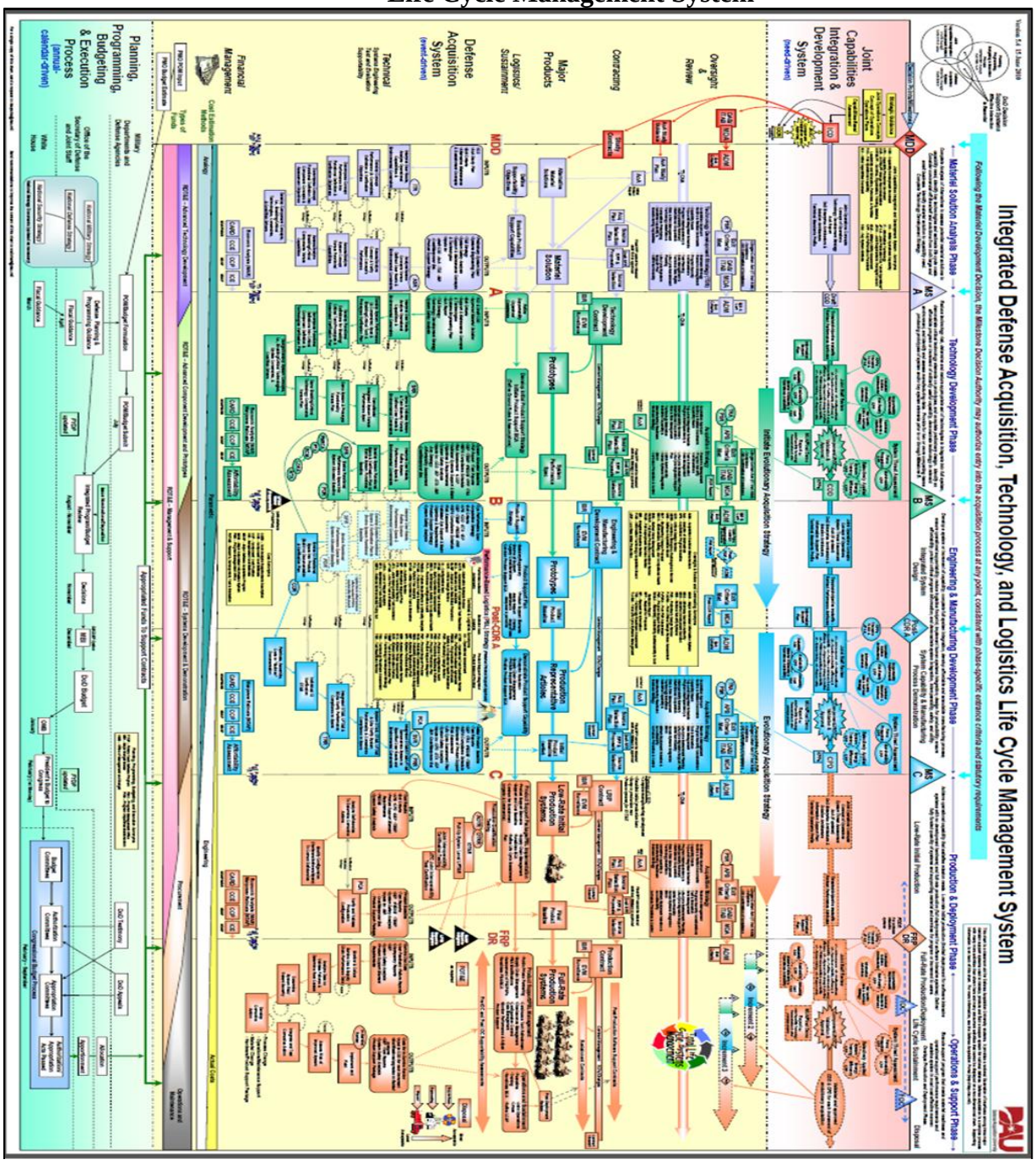
Appendix B –

Anti-Tamper Reference Timeline



Appendix C –

Life Cycle Management System



Appendix D –

Anti-Tamper Implementation Process