CVE-2014-0528
CVE-2014-0281
CVE-2014-6545
CVE-2014-0124
Java
CVE-2014-0617
CVE-2014-1156
CVE-2014-2121
ERROR
CISCO

Keywords: *DoD, Acquisition, Vulnerability Market, Reverse Auction, Metric*

Strengthening DoD Cyber Security with the Vulnerability Market

Maj Bradley C. Panton, USAF, John M. Colombi, Michael R. Grimaila, and Robert F. Mills

Every year, the Department of Defense (DoD) upgrades its information technology systems, allows new applications to connect to DoD information networks, and reconfigures the enterprise to gain efficiencies. While these actions better support the warfighter and satisfy national security interests, they introduce new system vulnerabilities waiting to be exploited. Often, these vulnerabilities are discovered only after the system has already deployed, where costs to fix are much larger. This article recommends the DoD adopt an economic strategy called the vulnerability market, or the market for zero-day exploits, to enhance system Information Assurance. Through the mutual cooperation between industry and the military in securing information, the DoD optimizes security investments, secures critical information, and provides an effective and resilient warfighting capability.

« Image designed by Diane Fleischer

To save money, increase automation, and facilitate information sharing, the Department of Defense (DoD) is increasingly acquiring new information system(s), or IS. These new systems are more complex, interconnected, and interdependent than older systems in the DoD inventory. With these new capabilities comes a negative externality; the more complex a system is, the more difficult it is to secure. Faced with this reality, the United States is making a significant investment in cyber security. In the years between 2004 and 2009, the annual federal cyber security investment grew from $4.2 billion to $7.3 billion (a 58 percent increase). The augmented investment in cyber security focuses on establishing a front-line defense to prevent intrusions, integrating intelligence into cyber security, and shaping the future environment by enhancing research, development, and education. One gaping hole in this strategy is a focus on acquiring systems that are secure by design. This article is an analysis of that gap and investigates whether the integration of a vulnerability market (VM), or the market for zero-day exploits, increases overall DoD cyber security and lowers the total cost of ownership for acquired systems.

The Prevalence of Vulnerabilities

Historically in the DoD, as budgets get tighter, IS aggregate. This phenomenon occurs primarily to offset the expense of maintaining a large workforce by automating much of the work accomplished by individuals. These systems also aggregate because of technological advances that reduce their physical footprint and required operations and maintenance (e.g., virtualization). As a consequence of aggregation, an increase in the number of automated processes drives an increase in the quantity and complexity of IS. Unfortunately, as the number, complexity, and size of systems increase, the prevalence of flaws also increases.

A common measure of the complexity of a system is calculated by enumerating the amount of software lines of code (SLOC). In 2010, a RAND study noted large code bases typically indicate a rate of one defect for every thousand lines of code (Landree, 2010). By applying this defect rate to two widely utilized operating systems—Windows Vista and Debian Linux—there would be approximately 50,000 defects in the Microsoft Windows Vista Operating System, and 200,000 defects in Debian Linux (Marchenko & Abrahamsson, 2007). Applying this defect rate to the Navy DD(X)'s 10 million SLOC, there may be as many as

10,000 defects. While only a fraction of these defects would allow access to the IS and lead to unauthorized system control, an entirely defect-free IS is realistically impossible to achieve.

DoD's Information Security Efforts

In response to the enormity and potential consequences of a state-sponsored or independent hacker exploiting critical system vulnerabilities, the DoD relies on a concept called "Defense-in-Depth." Defense-in-Depth is the DoD approach to distributing system-wide exploitation risk across multiple levels of information security. The levels integrated in this shared-risk environment, according to Department of Defense Directive (DoDD) 8500.01E, are: "people, technology, and operations; the layering of IA [information assurance] solutions within and among IT [information technology] assets; and, the selection of IA solutions" (DoD, 2002). Stated simply, by applying information security tools across multiple boundaries of the DoD enterprise, exploiting a vulnerability at the interior of the network is increasingly difficult.

In the cyberspace domain, exploiting a system can be categorized as targeted or indiscriminate. Indiscriminate attacks are those not focused at a particular entity; rather, they seek to exploit security vulnerabilities across many systems. These attacks are often thwarted by several layers of the DoD enterprise network security as the level of system fingerprinting and malware complexity is limited and easily recognized. On the other hand, a targeted attack is executed by a highly skilled individual(s) who seek to attack a specific system. Because the target is specific, the attacker will become an expert on its network architecture, hardware and software components, and intrusion safeguards.

As layers of network defense increase, attack sophistication grows as well. According to an October 2011 report released by the U.S. Government Accountability Office (GAO), 20 federal agencies reported an increase in the amount of targeted and indiscriminate cyber attacks against critical assets. In fact, these agencies (one of which was DoD) reported a 25 percent increase in the number of reported intrusions from 2009 to 2010 (GAO, 2011). Unlike a medieval castle where an enemy can defeat a single layer of defense without compromising the entire castle, cyber security is defeated if a single available attack vector is successfully identified and exploited.

In November of 2007, the DoD established the *DoD Information Assurance Certification and Accreditation Process (DIACAP)* policy, captured in Department of Defense Instruction (DoDI) 8510.01 (DoD, 2007). The purpose of DIACAP is to provide a risk management process for IA and detail IS certification and accreditation requirements throughout a system's life cycle. It provides a step-by-step process to assure DoD systems are protected and defended "by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation" (DoD, 2002). DIACAP was created out of necessity as the former policy, DITSCAP (DoD Information Technology Security Certification and Accreditation Process), was ill-equipped to handle information systems in the net-centric environment. Improving upon DITSCAP, DIACAP established standardized IA controls, a schedule to review an individual system's IA status, and testable metrics to measure security effectiveness. Although this is seen as an improvement over DITSCAP, DIACAP has flaws.

DIACAP measures security effectiveness according to a prescribed timeline (every 1 to 2 years). Should a new vulnerability be discovered, verification of a security patch installation could then take months before the next IA inspection. Furthermore, the IA controls monitor known system vulnerabilities and do not take into account threat monitoring, incident detection, or incident response. DIACAP is a risk mitigation process that is more reactive than proactive when it comes to system vulnerabilities. It works well for new IS acquisitions as they are tested against the latest vulnerability database with the latest tools. As systems mature, DIACAP becomes less effective as threat monitoring takes a back seat to operations. Currently, efforts are underway to revise how the DoD handles certification and accreditation of its systems. These efforts are resulting in a revision of the DoDI 8500.02 series, which will mandate the use of the DoD Information Assurance Risk Management Framework (DIARMF). While DIARMF addresses many shortcomings, it will be years before the process is fully implemented.

Penetration testing, or authorized hacking, is designed to evaluate the vulnerability of a system to indiscriminate and targeted cyber attacks. The goal of penetration testers is to obtain unauthorized privileges by exploiting flaws in system design or implementation (Chairman of the Joint Chiefs of Staff Instruction [CJCSI] 6510.01, 2011). Other incidents that penetration testing detects include denial of service, malware

infection, and malicious code. Unfortunately, penetration testing can never prove a system is void of vulnerabilities. Penetration testing only identifies the presence of known vulnerabilities.

Following the fielding decision for new information systems, organizations schedule periodic red and blue team penetration exercises to test system security. These tests prove effective across the entire DoD network; however, team manpower makes it difficult to assess the majority of systems. In an effort to offset the manpower shortfall, the DoD is embarking on the development of several "cyber test ranges" to simulate real-world conditions in a controlled environment. Two such environments in development are known as the DoD Information Assurance Range and the National Cyber Range.

The assemblage of the DoD defense-in-depth strategy—DIACAP framework, penetration test tools, and cyber test ranges—represents the government's dedication to identify known system vulnerabilities. Even with these monumental fiscal and personnel investments, the DoD remains incapable of measuring the security of a system with a meaningful metric.

Vulnerability Markets

Prior to 1997, the Federal Acquisition Regulation (FAR) prohibited use of auctions to establish contracts between the government and supplier. Language in the FAR specifically prohibited auction techniques that indicate to an offeror a cost that it must meet to obtain further consideration; advise an offeror of its price standing relative to another offeror; and otherwise furnish information about other offerors' prices (General Services Administration [GSA], 2005, pt. 15.610[e][2]). In 1997, the FAR was rewritten, and the Office of Management and Budget (OMB) removed the ban on government involvement in auctions. Ever since, DoD has taken advantage of the e-commerce auction marketplace to procure a variety of supplies. Some examples of DoD auction procurements include:

- Navy procuring aircraft and ship parts;
- Army purchasing IBM ThinkPads, saving 40 percent off the GSA price;

- Army purchasing spare parts for the Patriot Missile system; and

- Air Force acquiring computer equipment, saving 27 percent.

Additionally, the OMB reported that the Environmental Protection Agency conducted 94 reverse auctions in 2007 and saved almost 14 percent from the government estimate (OMB, 2008). In tight fiscal times, where saving money is the lifeblood of any program, the savings achieved by using online auctions are hard to ignore. Although these auctions have only been employed for the procurement of physical items, the model is applicable toward purchasing software security vulnerabilities in the cyber domain.

Vulnerability Market Examples

The VM emerged as a way for security researchers and hackers to disclose vulnerabilities for financial gain. In the past decade, three VM models surfaced, which form the majority of vulnerability events: the bug challenge, the bug bounty, and the bug auction.

Bug Challenge

In a bug challenge, the simplest of the VM models, a vendor offers a reward for reporting vulnerabilities related to a particular product. Unlike the other two models described in this section, the bug challenge is administered directly by the vendor and has no intermediary acting as a clearinghouse. This model has a couple of major flaws. First of all, prizes for a vulnerability are not market-driven and may not accurately reflect its actual value (Schwalb, 2007). As finding vulnerabilities involves a significant investment, researchers could sell their finds on the black market for a much higher price. Secondly, bug challenges are often by invitation-only, where the researchers are placed on contract and required to sign nondisclosure agreements. By restricting the researchers, the vendors have the ability to keep any vulnerabilities secret and subsequently refuse to patch the products.

For 3 weeks in 2000, the Secure Digital Music Initiative (SDMI) conducted a public bug challenge aimed at breaking SDMI watermarking technologies. The challenge was invitation-only and offered a cash prize for any team that could win any of the six challenges posed. The ultimate goal was to identify an authentic copy of the audio file to combat online

music piracy. This event was sanctioned by the music recording industry and required all participants to sign a nondisclosure agreement prior to accessing SDMI data files (Craver, 2001).

Bug Bounty

Differing from a bug challenge, a bug bounty is conducted by a vendor seeking to pay researchers to identify malicious code used to infiltrate their systems. The goal of this market model is for a vendor to flush out an undetected vulnerability currently being exploited by hackers. Placing a bounty on vulnerabilities is, by nature, a reactive countermeasure to unsecure software. Recognizing the benefit of this model, the company that developed the popular Web browser Mozilla instituted the Mozilla Security Bug Bounty. Starting in 2004, the Bug Bounty sought to reward individuals who reported *critical* security bugs (The Mozilla Foundation, n.d.). Since December of 2010, Mozilla has paid out a total of $104,000 for 64 qualifying bugs.

Bug Auction

A bug auction utilizes auction theory to conduct a VM. Conducted in an online environment, sellers of vulnerabilities attempt to maximize profit while buyers attempt to minimize cost. In bug auctions, two models are commonly used: the English and Dutch auctions, described in Table 1.

TABLE 1. DESCRIPTION OF COMMON AUCTION TYPES

Auction Type	Bidding / Offer Process	Description
English (Traditional)	Bids increase	This is the typical auction in which a single seller of a single item (or lot of items) receives increasing bids from prospective buyers. The auction ends at a predetermined time, and the item goes to the highest bidder for the highest bid price.
Dutch (Reverse)	Offers decrease	The exact opposite of the English auction. A single buyer of a single item (or lot of items) receives decreasing offers from prospective sellers. The auction ends at a predetermined time, and the item is purchased from lowest offerer for the lowest price.

Note. Adapted from "Auctions in Defense Acquisition: Theory and Experimental Evidence," by B. Linster and D. Mullin, *Acquisition Review Quarterly*, Summer 2002, p. 214.

In contrast to the widely used English auction, Dutch (Reverse) auctions are less frequently utilized. Reverse auctions, consisting of one buyer and multiple sellers, are occurring more frequently in government material acquisitions. While not yet applied to information security, several federal agencies recognize the financial benefit of market competition between suppliers. Several cases of successful reverse auctions are detailed in Table 2.

TABLE 2. HISTORIC SAVINGS FROM COMMERCIAL AND GOVERNMENT REVERSE AUCTIONS

Procuring Activity	Item Procured	Cost Savings	% Savings
State of Pennsylvania	Aluminum	$170,000	9%
United Technologies	Circuit Boards	$32,000,000	53%
Owens Corning	Packing Materials	$7,000,000	7%
U.S. Navy (NAVCIP)	Ejection Seat Components	$933,000	28%
U.S. Air Force	Computers	$88,000	27%
DESC	Natural Gas	$972,000	22%
U.S. Army CECOM	Transformers	$195,000	53%

Note. Adapted from CLC031: *Reverse Auctioning* [Online course module], published by the Defense Acquisition University, 2012. NAVCIP = Naval Inventory Control Point; DESC = Defense Energy Support Center; CECOM = Communications-Electronics Command.

Reverse auctions may benefit DoD information security in three ways. First, reverse auctions enhance cyber security through early identification of vulnerabilities. Second, the auctions leverage the skills and knowledge of private security researchers in the private sector. Third, when compared to an expected loss, executing an auction costs far less than remediating an attack.

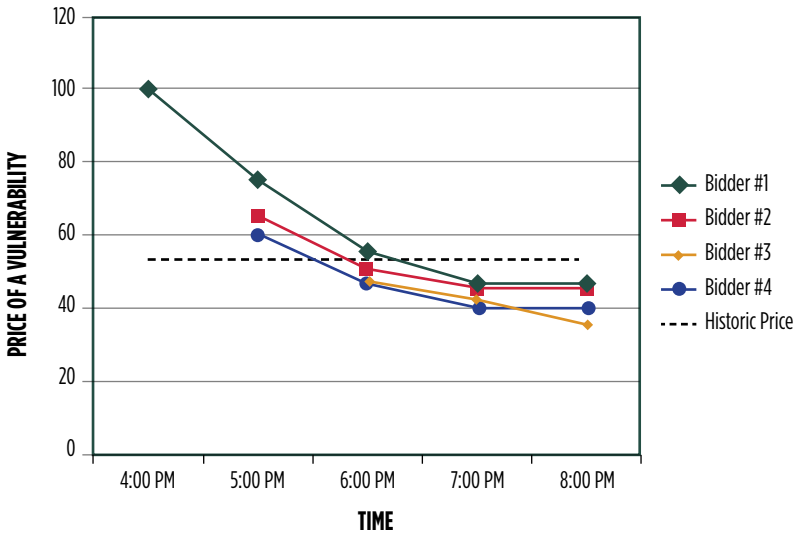
Based on these advantages, this article concentrates on developing a reverse auction model to be used by the DoD prior to full system deployment.

Applying Reverse Auctions

While traditional auctions aim to increase bids on an item for sale, reverse auctions strive for the opposite: to drive prices down. In reverse auctions, buyers initiate the auction rather than the seller. The buyers identify a product or service they want to buy and the starting price at which they are willing to compensate the sellers. Once the auction

window is opened, the bidders (e.g., the sellers) compete to offer the products or services at the lowest cost possible while still retaining a profit. This concept takes advantage of free market competition to lower prices for the buyer (Figure 1).

FIGURE 1. REVERSE AUCTION—PRICE DRIVEN DOWN OVER TIME

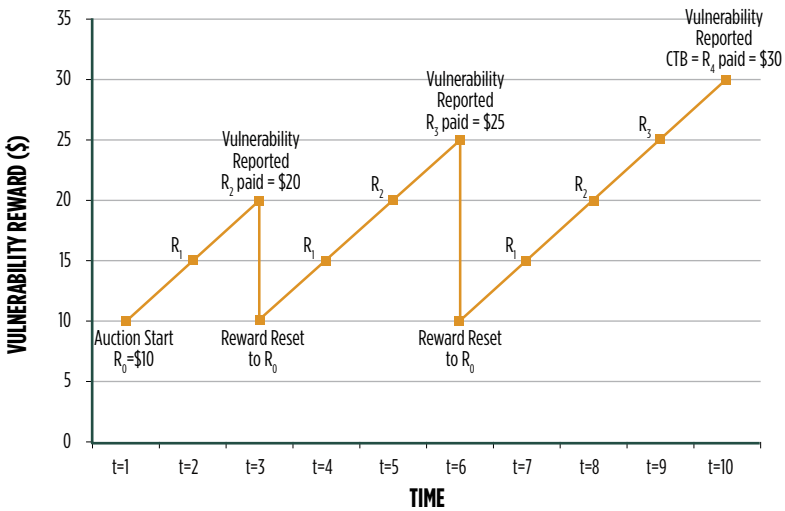


The purpose of using a reverse auction to discover vulnerabilities is twofold. The first objective is to identify possible security issues associated with a software product. By offering cash incentives, vulnerability discovery rates increase based upon the number of researchers attracted to the competition. The greater the number of researchers, the more likely a vulnerability will be found. The second objective is that the vulnerability auction has the potential to provide a meaningful metric that would describe the relative security of a product.

Using a variant of the reverse auction model will allow the government to use auctions for the procurement of software vulnerabilities. The government (aka the buyer) would initiate a reverse auction within an identified pool of software researchers (aka the sellers). The government would identify and provide access to a system it believes to be secure. The government's certainty of system security is articulated as an initial monetary valuation, expressed as the variable R_0. The objective of the researcher participating in the auction is to disprove the government's

assertion. If after a predetermined amount of time a researcher does not report a vulnerability to the government, the reward value increments from R_0 to R_1. In the Figure 2 example, the reward first increments from R_0 = \$10 to R_1 = \$15. This incremental increase repeats until a vulnerability is reported or until the prearranged auction window closes. R_n represents the amount (\$) of reward at increment "n." If a researcher reports a software vulnerability, the government would pay the current value of R_n dollars. The Figure 2 example shows vulnerabilities reported at R_2 and R_3 where a researcher is paid \$20 and \$25, respectively. At the auction's conclusion, the last value of the reward (R_4), equates to the security of the system. This final value, or the Cost-To-Break (CTB) metric, is the amount of money it costs an individual to discover and report a vulnerability.

FIGURE 2. REVERSE AUCTION–REWARD OVER TIME, UP TO COST TO BREAK (CTB)



Applying VM Concept to DoD Information Systems Acquisition

For the DoD VM to be successful, it is imperative that a substantial set of qualified software researchers participate. As arduous as it is to discover software vulnerabilities, the researchers must perceive an adequate level of compensation for their efforts. Compensation to incentivize participation can take many forms in the VM.

Financial gain is the most common type of incentive offered in commercial VMs. In March 2012, *Forbes* published a price list that enumerates the financial value an open market vulnerability possesses (Table 3). The value of these vulnerabilities is a function of a free-market economy and the forces of supply and demand. While the vulnerability may not be worth the cost to the vendor, potential consumers of vulnerabilities may perceive the cost offsets their risk and any potential costs of using the vulnerability.

TABLE 3. PRICE LIST FOR SOFTWARE VULNERABILITIES

Application	Vulnerability Price List
Adobe Reader	$5,000 – $30,000
MAC OSX	$20,000 – $50,000
Android	$30,000 – $60,000
Flash or Java Browser Plug-ins	$40,000 – $100,000
Microsoft Word	$50,000 – $100,000
Windows	$60,000 – $120,000
Firefox or Safari	$60,000 – $150,000
Chrome or Internet Explorer	$80,000 – $200,000
iOS	$100,000 – $250,000

Note. Adapted from "Shopping for Zero-Days: A Price List For Hackers' Secret Software Exploits," by A. Greenberg, 2012, *Forbes*.

To establish a financial reward, the DoD must provide additional reassurances in the form of nonattribution and anonymity to the researchers. Nonattribution and anonymity have a value unto themselves. By offering a safe and nonattribution environment, security researchers are welcome to hack a government system without threat of being prosecuted under state and federal law. These reassurances, coupled with a financial reward, must counterbalance the price of a vulnerability on the open market.

In the world of vulnerability discovery, a major motivation amongst researchers is their reputation. In the hacker community, an individual's reputation ranges from the lowest revered status of "script kiddie" to the highest "elite" status. John Arquilla, a professor of defense analysis at the U.S. Naval Postgraduate School in Monterey, California, recently estimated that only around 100 "elite" hackers are in the world today (Carroll, 2012). By leveraging reputational exclusivity and the egos of

security researchers, the DoD could incentivize individuals to participate. A researcher's reputation may be elevated based upon the number of vulnerabilities or new attack vectors discovered. A heightened reputation will enhance the researcher's status in the hacker community and could also result in job and consulting offers within industry.

Altruism, in the cyber security environment, is also a powerful motivator. It is so powerful, in fact, that the term "white hat" hacker was developed specifically for the altruistic security movement. The term white hat describes a hacker ethically opposed to the abuse of IT and concerned with improving overall security to benefit society. Traditionally identified as specialists in penetration testing or vulnerability investigation, white hats use their expertise to protect computer health and improve system security. After discovering a vulnerability, white hats will either contact the vendor directly to force a patch or disclose the vulnerability to a third party like the United States Computer Emergency Readiness Team. These incentives, with cash rewards resulting from a DoD-sponsored VM, have the propensity to increase software vulnerability discovery rates and software security.

Cost to Break

Complete product security is almost impossible to measure. Metrics, such as SLOC, can describe complexity of the system, but fail to describe overall security. The number of vulnerabilities patched over a given amount of time is also a useful metric that is quantifiable and easily understood. Moreover, a company can advocate the amount of effort (in dollars and time) spent securing a product. The failure of this metric is that a hacker only needs a single undiscovered vulnerability to exploit the system. To provide a meaningful way of measuring the security of a system, the DoD requires a metric that is quantifiable, easily understood, dynamic, and supports IT acquisition milestones for decision makers.

The traditional definition of a system's CTB is the cost that an attacker will incur in compromising the system. These costs may include money, research time, risk of being caught, etc. Because many of these costs truly vary amongst individuals, calculating this view of the CTB metric is unfeasible. Rather than attempting a CTB metric focused on the individual, this article proposes using the VM to evaluate the security of the system by using a large sample population of security researchers.

Using a VM to calculate the CTB of a system was originally proposed by Dr. Stuart Schechter of Harvard University. In Dr. Schechter's model, the CTB is the result of the market price to discover system defects governed by the presence of competition amongst researchers (Schechter, 2002). Otherwise stated, the market-focused CTB is a product of a vulnerability auction where an IT producer offers a cash prize to free-market researchers to break their system. This strategy of paying researchers to break their systems is used frequently today; however, it is not tracked as a true metric. For example, since 2007 the CanSecWest security conference has hosted the annual Pwn2Own bug challenge, which rewards researchers for hacking into some of the most popular computer applications. During the 2013 Pwn2Own challenge, researchers were awarded $480,000 for cracking applications developed by Microsoft, Google, Adobe, Mozilla, and Oracle. Even more impressive, Google claimed theirs was the most secure operating system on the market by offering $110,000 for a browser or system-level compromise delivered via a Web page. At the end of the conference, the entire Google prize pot of $3.14 million remained intact (Thomson, 2013).

The inability of researchers attending the conference to crack the application effectively placed the CTB metric for the Google Chrome OS at $110,000. Accordingly, this metric could be used by Google to compare its security to other operating systems (e.g., Windows, Linux). This ability to compare applications is the real value of the CTB metric; the vendor is now able to highlight the security of its product relative to its competitors. For a discerning consumer concerned with product security, the CTB may influence the decision to purchase one product versus another.

The CTB metric may play a role in the DoD as well. Prior to awarding a contract to a specific vendor, the DoD establishes a source selection strategy or acquisition plan that outlines all evaluation factors affecting contract award. Should software security be an evaluation factor in the selection, the CTB would be invaluable in the comparison of multiple vendors. The hope would be that the DoD acquires secure software systems prior to contract award. Additionally, use of the CTB metric could be included in the Joint Capabilities Integration and Development System requirements process. By requiring that an IS must meet specified thresholds, the contractor and government ensure the IS is secure prior to deployment.

Application of a VM leads to several benefits. First of all, a VM provides an additional round of development and operational testing. Second, the VM increases analysis prior to fielding. Increased scrutiny and additional researchers also increase the vulnerability disclosure rate and result in reducing the total cost of ownership. Third, by wide use of the VM to enumerate the CTB metric, the government will be able to compare and discern multiple systems.

Conclusions and Recommendations

Perfect information security will never be achieved. Whether vulnerabilities are due to mistakes by the software developer, a vendor's unwillingness to fix flaws, or an error by the user, the outcome is the same—valuable information is susceptible to attack. In the information age, industry understands the issues of software vulnerability prevalence as much as the DoD. In the past decade, dozens of VMs have sprung into existence based upon the perceived need to enlist nonorganic researchers to report application vulnerabilities. The responsibility for securing data does not lie solely with the vendor or with the product consumer. True information security and management of the risk of unauthorized disclosure is the responsibility of the entire community.

Because a government online reverse auction market for the purpose of identifying software vulnerabilities has never been applied to a DoD IS acquisition, concerns arise that this concept is legally and economically unfeasible. Legally, federal statute permits and encourages the use of online marketplaces (GSA, 2005, pts. 1.102, 4.5) for systems acquisition. Furthermore, precedent in the commercial and government sectors is established. As reported by the *Washington Post*, the National Security

Agency (NSA) allegedly spent more than $25 million in 2012 to procure vulnerabilities (Fung, 2013). With respect to security concerns, the National Institute of Standards and Technology encourages acquiring systems that are "secure by design" rather than those that are "secure by obscurity." While obscurity and controlling open visibility into systems design might delay potential adversaries, hidden vulnerabilities may ultimately be exploited to their advantage. Security by design does not rely on hiding vulnerabilities. Instead, vulnerabilities are eliminated by secure software design principles. In cases where a critical system must be controlled and disseminated to trusted individuals, entry into the VM is governed through the enforcement of appropriate clearance requirements.

Economically, each IS vulnerability has the probabilistic potential to cost the DoD immense resources. Although calculating the consequences of using a system with unknown vulnerabilities is difficult to quantify, discovery of a vulnerability prior to use in an operational environment is more cost-effective than remediating it postdeployment. Decreasing the probability and increasing the discovery rate of system vulnerabilities are the primary goals of the proposed VM model for DoD-acquired systems. Not only will the discovery of an unknown vulnerability effectively reduce the probability of a successful attack, life-cycle operations and maintenance costs are also reduced. Addition of a VM to the development phases within DoD acquisition results in a proactive approach to information security and mission assurance.

Use of this auction model will create a meaningful and easily understandable metric to ensure the DoD acquires systems with built-in security. This CTB metric has the propensity to reform the defense industrial base as well as conform to information security requirements as dictated by the warfighter. Through the mutual cooperation between industry and the military in securing information, the DoD will optimize security investments, secure critical information, and provide an effective and resilient warfighting capability.

Author Biographies

Maj Bradley C. Panton, USAF, is currently an acquisition program manager at the U.S. Cyber Command. As a program manager, Maj Panton has worked at the U.S. Air Force Electronic Systems Center, the Missile Defense Agency, and the National Geospatial-Intelligence Agency. He is Defense Acquisition Workforce Improvement Act-certified at ACAT Level III in Program Management. Maj Panton holds a BS in operations research from the U.S. Air Force Academy, an MS in military operational arts and sciences from Air University, and an MS in cyber warfare from the Air Force Institute of Technology (AFIT).

(E-mail address: bcpanto@cybercom.mil)

Dr. John M. Colombi is an assistant professor of Systems Engineering at the AFIT. He teaches graduate courses and leads sponsored research in support of the Systems Engineering program. Before joining the faculty, he led Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems integration activities, including systems engineering for the Airborne Warning and Control System. Dr. Colombi served at the National Security Agency developing information security and managed communications networking research at the Air Force Research Laboratory. He holds a PhD from the AFIT.

(E-mail address: john.colombi@afit.edu)

Dr. Michael R. Grimaila is an associate professor of Systems Engineering and Management and member of the Center for Cyberspace Research at the AFIT, Wright-Patterson AFB, Ohio. He is a Certified Information Security Manager, a Certified Information Systems Security Professional, a member of the Association for Computing Machinery, a senior member of the Institute of Electrical and Electronics Engineers (IEEE), and a Fellow of the Information Systems Security Association. He holds a PhD from Texas A&M University.

(E-mail address: michael.grimaila@afit.edu)

Dr. Robert F. Mills is an associate professor of Electrical Engineering in the Department of Electrical and Computer Engineering, AFIT. He teaches and conducts research in a variety of areas, including cyber security, network operations and management, electronic warfare, and systems engineering. He serves as the curriculum chair for AFIT's Cyber Warfare master's program and is a senior member of the IEEE. He holds a PhD from the University of Kansas.

(E-mail address: robert.mills@afit.edu)

References

Carroll, R. (2012, July 10). US urged to recruit master hackers to wage cyber war on America's foes. *theguardian*. Retrieved from http://www.guardian.co.uk/technology/2012/jul/10/us-master-hackers-al-qaida

Chairman of the Joint Chiefs of Staff. (2011). *Information assurance (IA) and support to computer network defense (CND)* (CJCSI 6510.01F). Retrieved from http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf

Craver, S., Wu, M., Liu, B., Stubblefield, A., Swartzlander, B., Wallach, D., … Felten, E. (2001). Reading between the lines: Lessons from the SDMI challenge. *The USENIX Association*. Retrieved from http://static.usenix.org/events/sec01/craver.pdf

Defense Acquisition University. (2012). CLC031: *Reverse auctioning* [Online course module]. Retrieved from http://icatalog.dau.mil/onlinecatalog/courses.aspx?crs_id=440

Department of Defense. (2002). *Information assurance* (DoDD 8500.01E). Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf

Department of Defense. (2007). DoD *information assurance certification and accreditation process (DIACAP)* (DoDI 8510.01). Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf

Fung, B. (2013, August 31). The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities. *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities

General Services Administration. (2005). *Federal Acquisition Regulation*. Retrieved from http://www.acquisition.gov/far/90-37/html/15.html

Government Accountability Office. (2011). *Information security: Weaknesses continue amid new federal efforts to implement requirements* (Report No. GAO-12-137). Washington, DC: Author.

Greenberg, A. (2012, March 23). Shopping for zero-days: A price list for hackers' secret software exploits. *Forbes*. Retrieved from http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits

Landree, E. (2010). *Implications of aggregated DoD information systems for information assurance certification and accreditation*. Santa Monica, CA: RAND.

Linster, B., & Mullin, D. (2002, Summer). Auctions in defense acquisition: Theory and experimental evidence. *Acquisition Review Quarterly*, 212–223.

Marchenko, A., & Abrahamsson, P. (2007). Predicting software defect density: A case study on automated static code analysis. *Agile Processes in Software Engineering and Extreme Programming.* Berlin: Springer.

Office of Management and Budget. (2008). *Effective practices for enhancing competition* [Memorandum]. Retrieved from http://www.whitehouse.gov/sites/default/files/omb/procurement/memo/enhancing_competition_071808.pdf

Schechter, S. (2002, October). How to buy better testing: Using competition to get the most security and robustness for your dollar. *Infrastructure Security Lecture Notes in Computer Science*, 2437, 73–87.

Schwalb, M. (2007). Exploit derivatives & national security. *Yale Journal of Law and Technology, 9(1)*, 161–192.

The Mozilla Foundation. (n.d.). *Mozilla*. Retrieved from https://www.mozilla.org/en-US/foundation/

Thomson, I. (2013, March 8). *Pwn2Own: IE10, Firefox, Chrome, Reader, Java hacks land $500k*. Retrieved from http://www.theregister.co.uk/2013/03/08/pwn2own_contest_cansecwest/