Emerging Economic Models for Vulnerability Research

Michael Sutton, CISSP
Director, iDefense Labs
iDefense, A VeriSign Company

Frank Nagle, CISSP
Asst. Director, Vuln. Aggregation Team
iDefense, A VeriSign Company

Table of Contents

1 Introduction

The purpose of this paper is to look at economic vulnerability models that exist in the market today and analyze how they affect vendors, end users and vulnerability researchers. This paper attempts to draw upon previous research in this domain, but unlike papers such as those by Kannan *et al.*[1] and Nizovtsev *et al.*[2], this work is based on models that already exist in various markets rather than theoretical models. The authors' positions as employees of a company operating in this market space provide a unique perspective and valuable insight into all of the covered markets and models. The markets addressed include the government market, open market, underground market, auction market (which has yet to fully develop) and vendor market. Within the government market there are three models: internal discovery, contracted research and the purchase of externally discovered vulnerabilities. The open market is comprised of the outsourcing model and the internal discovery model. The underground consists of models similar to the government space with contracted research and the purchase of externally discovered vulnerabilities. The auction market can be considered its own model, as proposed by Andy Ozment[3], but is highly theoretical for reasons that will be discussed later. The final market, vendors, is unlike the other four markets for reasons that will be explored through the compensation and no compensation models. In writing this report, we first define each of these models, including their expenses, revenues and challenges. We then investigate the impact and implications of each model on vendors, end users and vulnerability researchers. Finally, we examine how each of the models affects these various actors and project the future of the market to see how the models that exist today will help to shape and drive the future of vulnerability research.

2 Economic Vulnerability Models

2.1 Government

Many governments have formal programs in which non-public vulnerabilities that can be used in offensive and defensive security are highly sought after. These vulnerabilities may be discovered by internal research teams or obtained from third parties. While this paper focuses primarily on the practices of US government agencies, there is evidence that information warfare programs exist among many national governments. A 2004 report published by the Institute for Security Technology Studies at Dartmouth College[4], speculates that countries such as China, India, Iran and Russia have invested heavily and established capable nation state cyber warfare operations. Furthermore, a 2001 study published by the US Department of Defense[5] reported that “in excess of 20 countries already have or are developing computer attack capabilities.”

[1] Kannan, Telang, Xu. *Economic Analysis of the Market for Software Vulnerability Disclosure.*
[2] Nizovstev, Thursby. *Economic Analysis of Incentives to Disclose Software Vulnerabilities.*
[3] Ozment. *Bug Auctions: Vulnerability Markets Reconsidered*
[4] Billo, Chang. *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States*
[5] Defense Science Board. *Protecting the Homeland: Report of the Defense Science Board Task Force on Defensive Information Operations 2000 Summer Study Volume II*

When revenues and expenses associated with vulnerability discovery for government and commercial entities are compared, a clear difference exists on the revenue side of the equation. While commercial entities seek vulnerability information for economic gain, governments are motivated by national security. On the expense side of the equation, governments incur similar costs to their commercial counterparts. Governments seem to be very willing to pay labor costs in order to obtain the information they are seeking. Those costs come in the form of salaries for highly skilled employees or through outsourcing. The greatest challenge facing governments appears to be obtaining adequate human resources to conduct research. Governments generally have a smaller hiring pool of already scarce talent from which to select due to stringent and often time consuming background checks. However, this challenge can be partially overcome by outsourcing research to private contractors.

2.1.1 Internal Discovery

While governments typically do not advertise that they pay researchers to discover private vulnerabilities, it is not difficult to uncover evidence that such activity occurs. For example, the careers page on the NSA web site[6] clearly illustrates that the government is looking for such researchers. Under the 'Career Paths in Computer Science' heading, it clearly states that 'Vulnerability Discovery' is a defined job within the agency (Figure 1).

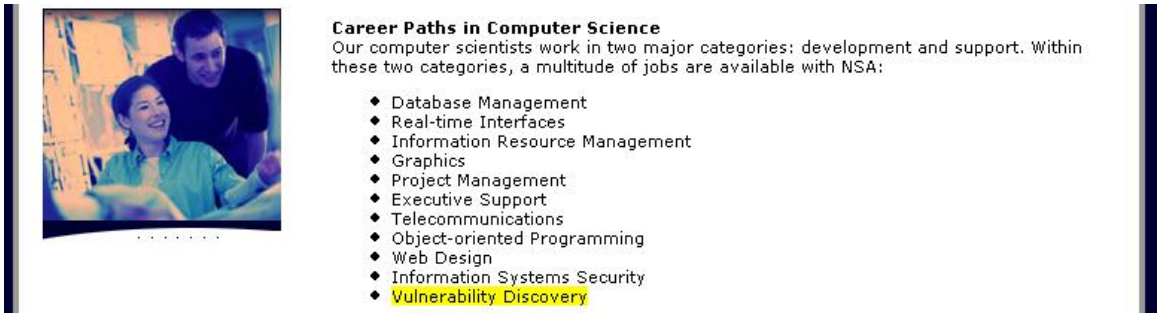

Figure 1 - NSA Job Posting

2.1.2 Contracted

While not widely publicized, evidence exists that suggests that vulnerability discovery is not solely done by internal researchers, but is also contracted out to third parties. Excerpts from publicly available documents provide insight into the process. For example, in a transcript from a July 22, 2003 committee hearing for the House Select Homeland Security Committee[7], Daniel G. Wolf, The NSA's Director of Information Assurance, discusses how part of his "mission statement is to discover vulnerabilities" and that such work is done "very closely with

[6] NSA Careers Website. http://www.nsa.gov/careers/careers_5.cfm
[7] House Select Committee on Homeland Security. *The Importance of Research in Cybersecurity and What More Our Country Needs To Do*

industry…and with academics." Additionally, an excerpt from the *Report of the Defense Science Board Task Force on Defensive Information Operations, Volume II*[8] states:

> *"The [Discover Vulnerabilities] (DV) process covers three levels of service. We believe the private sector can play a pivotal role in filling the Departments needs in the DV process where we (NSA, DoD Services, Agencies, etc) are over tasked and lacking, in some areas, skilled personnel. It is our sense that the [vulnerability assessments] and [vulnerability evaluations] process, where appropriate, can be assisted by the Defense contracting community if trained and certified appropriately."*

2.1.3 Purchase of Externally Discovered Vulnerabilities

We are not presently aware of any public evidence that governments directly pay for individual vulnerability discoveries made by researchers not under an existing contract. However, it is rumored that such activity occurs.

2.2 Open Market

There are numerous companies that buy and sell vulnerabilities on the open market. These constitute legitimate companies that either outsource their research efforts or hire full-time employees to discover vulnerabilities within specific products. There are various expenses and different revenue streams associated with the two different models. Within these models, most but not all of the companies who discover vulnerabilities disclose them to the affected vendors. Some companies also attempt to provide zero-day or private vulnerabilities to a select clientele. As such, they have no incentive to report vulnerabilities to affected vendors since patch availability diminishes the value of their product. Each of the different models has its own unique set of challenges, especially with regard to ethics and legality.

2.2.1 Outsource

Outsourcing models rely on contracting external researchers to discover vulnerabilities. The company obtains intellectual property (IP) rights to the vulnerabilities, then reports the issues to their clients and the affected vendor. Companies using the outsourcing model can be considered the same as Bohme's vulnerability broker.[9] Currently, only two companies publicly advertise this practice: iDefense, a VeriSign Company, and TippingPoint, A Division of 3Com. iDefense's Vulnerability Contributor Program (VCP)[10] and TippingPoint's Zero Day Initiative (ZDI)[11] openly employ the outsourcing model, encouraging security researchers to submit their vulnerability discoveries in exchange for monetary compensation. Both companies report that they responsibly disclose reported vulnerabilities to the affected vendors so they can fix the problem and provide an official patch. It should be noted that a third company, Digital

[8] NITS. *The Cyber Operations Readiness Triad (CORT)*
[9] Bohme. *Vulnerability Markets: What is the economic value of a zero-day exploit?*
[10] iDefense Labs VCP Website. http://labs.idefense.com/vcp.php
[11] TippingPoint ZDI Website. http://www.zerodayinitiative.com/

Armaments[12], started a similar program late last year, but it is unclear if they are an established entity since they do not advertise the sale of any product or service.

Outsourcing expenses vary and are driven by the number and type of submissions accepted. Neither company publicly advertises their pricing models; however they both advertise the availability of retention and reward programs aimed at gaining contributor loyalty. iDefense offers Incentive, Retention, Growth and Referral programs[13]. At the end of each quarter, the Retention Program rewards the past year's top five contributors with a share of a $30,000 bonus pool while the Incentive Program rewards the top three contributors of the quarter with a share of a $9,000 bonus pool. Individual payouts are as follows:

Ranking	Retention	Incentive
1st	$10,000	$5,000
2nd	$8,000	$3,000
3rd	$6,000	$1,000
4th	$4,000	
5th	$2,000	

The Referral Program rewards contributors for referring other contributors to the VCP with up to $1,000. Additionally, iDefense recently announced a new program with a $10,000 reward for finding a vulnerability in a Microsoft product that leads to a Microsoft Security Bulletin with a critical rating[14]. TippingPoint's reward program[15] is designed to be more like a frequent flyer program, rewarding individuals who accumulate sufficient ZDI Reward Points to be given bronze, silver, gold or platinum status. The platinum status includes a one-time bonus of $20,000, monetary and Reward Points increases per submission in the next calendar year and paid travel and registration for the DEFCON and BlackHat conferences in Las Vegas. Although the specific dollar amount paid for an individual vulnerability is unavailable, it is clear that both companies are willing to invest large sums of money to keep their contributors coming back.

The revenue streams for iDefense and TippingPoint vary greatly. iDefense gains revenue by directly reselling the information, while TippingPoint profits by offering exclusive protection against the vulnerabilities they purchase via their intrusion detection system (IDS) product. iDefense has a subscription-based service in which members pay to receive advanced notification about vulnerabilities and potential workarounds that can be used to mitigate the threat until the vendor releases a patch. iDefense's customer base is traditionally large financial institutions and government agencies that have significant security budgets. TippingPoint, on the other hand, does not directly sell the information to customers, but creates signatures for their IDS products so that their customers are automatically protected against exploitation of the vulnerabilities contributed to the ZDI program. TippingPoint has a range of products targeting mid-sized and large Fortune 500 clients. iDefense and TippingPoint do not rely solely on the VCP and ZDI programs for content. In addition to vulnerability reports based on information obtained through the VCP, iDefense also delivers reports on public vulnerabilities, malicious

[12] Digital Armaments Website. http://digitalarmaments.com/index.htm
[13] iDefense Labs VCP Rewards Program Website. http://labs.idefense.com/vcp_reward_programs.php
[14] Keizer. *Firm Offers $10K Reward For Critical Windows Bug*
[15] TippingPont ZDI Benefits Website. http://www.zerodayinitiative.com/benefits.html

code and geopolitical threats[16], while TippingPoint provides IDS signatures for public vulnerabilities and other potential threats[17].

There are three main challenges surrounding the outsourcing model within the open market: convincing security researchers to contribute vulnerabilities, gaining acceptance within the industry (including dealing with ethical issues) and developing a successful revenue model. The difficulty in addressing these three challenges is likely the reason why this model is presently only employed by the two companies mentioned above. Their programs thrive on the active participation of outside security researchers and, consequently, need a steady pool of contributions coming into their programs. Convincing security researchers to disclose details about their vulnerability findings and release the IP rights to these findings is not an easy task. Since the security research community is fairly small and tends to be highly concerned about privacy and anonymity, researchers must trust the people with whom they are working. Therefore, much of the recruiting for the VCP and ZDI is done through word of mouth. Both programs also advertise their programs at "hacker" conferences such as BlackHat and DEFCON by throwing parties for their current and potential contributors.[18]

The second challenge to this model is gaining acceptance within the industry and dealing with ethical issues. iDefense and TippingPoint have been highly criticized for their methods, which can include paying people that may be perceived as malicious "hackers."[19] Additionally, they have been questioned on ethical grounds for encouraging people to find vulnerabilities within products. Many product vendors do not see any value in this model, and gaining industry acceptance has not come easily.[20] The VCP is approaching its fourth anniversary, and during this time has dealt with numerous technology vendors. While many vendors now work closely with iDefense and attempt to address problems in a timely manner, there are others that publicly and privately criticize the program. TippingPoint's ZDI is less than one year old, and since it is seen as being very similar to the VCP, receives many of the same criticisms. To address the ethical concerns, both companies employ what they feel are "responsible disclosure" practices by reporting vulnerabilities to affected vendors, the waiting until the vendor releases a patch before publicly publishing details. Both the VCP[21] and ZDI[22] publish their disclosure policies.

The final, and perhaps most difficult challenge to address is how to develop a revenue stream from this model. Neither the VCP nor the ZDI provide for a specific revenue stream on their own. However, the attractiveness of the products offered by iDefense and TippingPoint are enhanced because they could help protect an organization against vulnerabilities before a vendor publicly fixes the issue. This lack of a well-defined revenue stream is most likely one of the greatest deterrents against other companies using this model.

[16] iDefense Basic Services Website. http://idefense.com/services/basic.php
[17] TippingPont Products Website. http://tippingpoint.com/products_dv.html
[18] Endler. *Announcing the Zero Day Initiative.*
[19] Evers. *Offering a bounty for security bugs*
[20] Gonsalves. *Microsoft Slams Security Firm's Bounty For Windows Flaws*
[21] iDefense VCP Disclosure Policy. http://www.idefense.com/legal.php (bottom of page)
[22] TippingPoint ZDI Disclosure Policy. http://www.zerodayinitiative.com/legal.html

2.2.2 Internal Discovery

The internal discovery model is similar to the outsourcing model; however instead of paying security researchers on a one-off basis, researchers are hired as full-time employees to discover vulnerabilities. There are fewer barriers to entry with this model. As a result, there are far more companies that employ this approach. Some companies specialize in particular products, such as databases, while others spread their efforts to a diverse set of products. Additionally, this model is used by a wide variety of companies, including companies as small as two to three people such as GLEG Ltd., Argeniss and Immunity, Inc. Mid-size companies such as Next Generation Security Software Ltd. and Secunia as well as larger companies such as Internet Security Systems Inc. (ISS), eEye Digital Security, iDefense and TippingPoint also employ this model. iDefense and TippingPoint are considered in this and the outsourcing category since both have lab functions staffed by full-time researchers tasked with vulnerability discovery.

Expenses vary from company to company, but this model relies on salaried employees, resulting in a variable cost driven by head count. At some of the smaller companies, where there are only a few employees, salaries depend directly on the revenue received through sales. Larger companies may have teams of up to a dozen researchers dedicated to discovering vulnerabilities. As individuals with the appropriate skills for vulnerability discovery research are somewhat scarce, the costs to hire and retain such individuals can be relatively high.

Revenue within the internal discovery model can be generated in ways similar to the Outsourcing model, either via a subscription-based feed or the sale of an IDS or IPS product. Subscription-based feeds sell access to the information, offering customers advanced notification regarding unpatched vulnerabilities. Product sales offer advanced protection or detection methods via proprietary signature files. Some companies use this model as the sole basis for their revenue, simply selling the rights to have advanced knowledge of the issue. Others use this model to augment other products and services and as a way of gaining publicity about their company when the issue is eventually patched by the vendor.

For the most part, subscription-based information feeds within the Internal Discovery model are similar to those within the Outsource model. However, unlike the Outsourcing model, some companies that implement the Internal Discovery model choose not to disclose their findings to the appropriate vendors. They do not disclose their findings to the vendor in order to increase their value as private information. Companies that apply this method tend to be small companies that sell a subscription to their information, such as Immunity, GLEG and Argeniss. Larger companies that use subscription-based services to generate revenue, such as iDefense, Secunia, ISS and NGSS, release vulnerability details to the appropriate vendor so that the issue can be addressed. Only after notifying the affected vendor do these companies release a public advisory about the issue.

iDefense, Secunia, ISS and NGSS have internal employees tasked with discovering and reporting vulnerabilities to the affected vendor. Each company generates revenue by selling a subscription that is based, at least in part on the advance notification of the vulnerabilities. Additionally, while not directly affecting revenue, the publicity and press coverage that results when one of these companies are cited as the discoverer of the vulnerability in a security advisory can help to

indirectly boost sales. Customers for this type of service usually include larger companies that wish to augment automated security measures with additional protections against unpatched vulnerabilities.
Immunity[23], GLEG[24] and Argeniss[25] are smaller companies that have internal employees who focus their efforts on discovering vulnerabilities. However, they do not report these vulnerabilities to the affected vendors. Subscribers to their product lines often receive exploit code for "zero day" vulnerabilities that have not been reported to the vendor. In these cases, the companies can extend the lifespan of a vulnerability by not disclosing it to the vendor. They may also have clients that benefit from knowledge of private vulnerability information. These methods are often criticized within the security community, but do not appear to be illegal because the information is sold with disclaimers saying that it should be used for testing internal networks, not breaking the law. Potential customers for these products could include customers attempting to protect and test their systems or customers using the exploits for offensive purposes.

TippingPoint, eEye and ISS all sell IPS, IDS and/or firewall products and increase the value of these products by using internally discovered vulnerabilities to create signatures and provide their clients with advanced protection. Revenue is generated primarily through product sales, but some of the companies also generate consulting revenue. They do not, however, directly sell information about the vulnerabilities themselves. Similar to the internal discoveries of the companies who sell subscription-based information services, these companies publish public advisories about their discovered vulnerabilities after the affected vendor has fixed the issue. Customers include small to large organizations. Since these products help to automate security protection, they tend to appeal to a broader customer base than pure subscription-based services.

There are three main challenges to the Internal Discovery model: guaranteeing a return on investment, developing a successful revenue model and dealing with ethical issues (especially the companies that do not report the vulnerabilities to the affected vendors). Vulnerability discovery is not always an exact science, and it is difficult to guarantee that someone hired to discover vulnerabilities will provide a positive return on investment. As noted above, vulnerability researchers are highly skilled and demand higher salaries. However, no matter how skilled the researchers, there is no guarantee that they will discover a sufficient number of vulnerabilities to recoup the company's investment. It is here where the outsourcing model is superior, as researchers are paid by the vulnerability, rather than provided a flat wage regardless of productivity. Additionally, outsourcing allows for the usage of researchers who might not be employable for reasons of citizenship, temperament, or any other reason.

Like the Outsourcing model, the Internal Discovery model faces the challenge of developing a significant revenue stream. Whether revenue is generated through a subscription-based service or through product sales, it can be difficult to determine exactly how much revenue the Internal Discovery team actually generates. Additionally, the value of the publicity and press gained from advisories released by the affected vendors that give credit to the discoverers cannot easily be measured. Companies that only report their discoveries to their customers and do not report the

[23] Immunity, Inc. http://immunitysec.com/index.shtml
[24] GLEG Ltd. http://www.gleg.net/index.shtml
[25] Argeniss Information Security. http://www.argeniss.com/index.html

issues to the vendor may actually face an easier time developing a revenue model. The argument that you could suffer a security breach if you don't buy their product can be compelling. Customers may simply pay for the information so that they can protect themselves against attacks or may intend to use it to launch attacks of their own.
The ethical issues surrounding the Outsourcing model also exist for the Internal Discovery model. For the most part, the Internal Discovery model is subject to fewer ethical criticisms than the Outsourcing model since the company is not generally perceived as paying hackers for their vulnerability information. However, companies that do not report their findings to the affected vendors walk a fine line. Should their exploits be used for illegal activities, could they be held liable? There doesn't appear to be any legal precedence to answer the question. Some of these companies are based in countries were computer security laws are less stringent and, therefore, might have some protection from legal action.

2.3 Underground

The underground market has similarities to the government and open markets. Like government and open markets, the underground market uses contracting and outsourcing models. However, the underground's focus is to inflict damage on or steal money from the general Internet society. Most underground activity occurs as either contracted work or purchased research. More simply, the market is split by those that pay vulnerability researchers to find specifically requested vulnerabilities, and those that pay for research and exploits already developed by a vulnerability researcher. While there is little public information on the contracted model, there is a very recent, very public example of the purchased model in action with the Microsoft Windows WMF rendering vulnerability, which was discovered by a vulnerability researcher and sold on the underground market to malicious actors.[26] Due to the discrete nature with which the underground market operates, it is rare that such an issue receives the kind of publicity this issue did. However, the WMF example does illustrate how the underground market model can be compromised. If the seller of the vulnerability sells it to someone who either goes to the vendor, or uses it in such a way that it is discovered and reported to the vendor by others, then the seller and all of the other buyers can no longer use the vulnerability.

2.3.1 Contracted

The contracted model involves a malicious actor (often related to an organized crime group) hiring a vulnerability researcher (often unaware of exactly who they are working for) to find vulnerabilities in a specific target. This target could be a particular software application, operating system or piece of hardware. The target could also be a specific corporate or government network that the malicious actor wishes to target. The malicious actor and the vulnerability researcher agree on a price and a particular deliverable, and the researcher attempts to find the specified vulnerability. Once a vulnerability is discovered, the researcher packages and delivers it according to the malicious actor's request.

Since there are two actors involved in this model, expenses must be discussed from the perspective of both sides. For the malicious actor, the expense involves the direct payment to the

[26] Microsoft Corp. Microsoft Security Bulletin MS06-001

vulnerability researcher and the expense of using the vulnerability to obtain the sought after objective. This expense might include paying others to use the vulnerability or time and money spent to find targets. For the vulnerability researcher, expenses involve the time needed to find the vulnerability and equipment (unless paid for by the malicious actor).

The revenue stream from this model is only limited by the imagination of the malicious actor. If the vulnerability that was found is in a widely deployed system, it could be used to power spam, spyware or adware; all of which can be used for monetary gain. For the most part, all of these activities are illegal. However, they are widely and effectively used. If the contract was for a more specific vulnerability in a particular system or network, then the revenue stream could also come through espionage or blackmail. These more targeted attacks can severely impact a particular person or company. Whether using spam, spyware or adware in a broader attack or using espionage or blackmail in a more targeted attack, there is an opportunity for vast financial gain.

The two main challenges to the contracting model are avoiding being caught by law enforcement and brokering the deal. To effectively use this model, both the malicious actor and the vulnerability researcher must be able to ensure that they will not be caught. It is for this reason that much of the activity appears to take place in countries with lax information security laws. That is why much of the "hacker-for-hire" industry is located in Brazil, Russia and the Ukraine rather than the United States or European Union. The challenge of brokering the deal arises due to concerns of the first challenge. There are numerous underground websites[27] and IRC chat rooms that are created specifically for putting malicious actors in touch with vulnerability researchers. Some even have places where malicious actors can post the vulnerabilities for which they are looking, allowing researchers to review them and decide whether they want to take the job.

2.3.2 Purchase

The purchase model is similar to the contracted model, except that it is done in reverse. In this model, the vulnerability researcher finds a vulnerability, creates an exploit and sells it to one or more malicious actors. This method is also similar to the variation of the Internal Discovery model within the open market where the vulnerability researcher does not report the vulnerability to the vendor, but only discloses the vulnerability to their customers. The largest difference between these two is that in the open market Internal Discovery model, the products are publicly marketed as tools for testing your own networks, while in the underground purchase model, the vulnerability and exploit are not publicly marketed, making it clear that the product will be used for malicious purposes. Underground transactions rarely appear in the public sphere, however the recent Microsoft Windows WMF issue was so severe that it was researched in depth. As a result of this research, information about the original transactions and the exploit code's sale price were uncovered.[28] For this reason, the WMF vulnerability will be used as an example when discussing the Purchase model.

[27] Web-Hack. http://web-hack.ru/
[28] Naraine. *Researcher: WMF Exploit Sold Underground for $4,000*

Since the Purchase model requires two actors, expenses for both actors must be assessed. As with the Underground Contracting model, the researcher's expenses involve time and resources needed to discover the vulnerability and create an exploit. Additionally, researchers must market their discovery in such a way as to attract the attention of malicious actors while avoiding law enforcement. The malicious actor's expenses are the price set by the researcher for the exploit and the cost of deploying the exploit in such a way as to generate sufficient monetary gain to cover the cost of buying the exploit. An obvious difference between the Purchase and Underground Contracting models is that malicious actors cannot dictate exactly what they want, they must be content to purchase what is available.
The researcher's revenue stream is directly dictated by their selling price and the number of purchasers. In the case of the WMF vulnerability, the researcher sold an exploit for $4,000 USD, and it is believed that they sold it to more than one malicious actor. The revenue stream of the malicious actor is similar to that of the same party in the Underground Contracting model. The malicious actor can use the exploit to power spam, spyware and adware, or to attempt to specifically target a person or company for espionage or blackmail. Again, the malicious actor's revenue stream is limited only by there imagination and the effectiveness with which they deploy the exploit. The WMF exploit was widely used on multiple malicious websites to spread spam, adware, spyware and other creative attacks. One malicious actor who purchased the WMF exploit used it to spread spam that promoted the stock of a Chinese pharmaceutical company in which they presumably already owned a great deal of stock. In a classic "pump and dump" scheme, they spread the spam via the WMF vulnerability to pump the stock and inflate its value for a few days. Once the value had increased, they dumped their shares and made quite a profit.[29]

The challenges faced in the Purchase model are the same as those faced in the Underground Contract model: avoiding capture by authorities and brokering a deal between the two actors. To solve the marketing and deal making challenges in the case of the WMF vulnerability, the actors most likely used an underground website to broker their deals.

2.4 Auction

While we are currently unaware of any auctions that have been established to trade vulnerability information, there is at least one occurrence of an attempt to sell vulnerability details on eBay[30]. The eBay auction involved the alleged sale of a vulnerability in Microsoft Excel, but was pulled by eBay officials who cited a violation in their policy of forbidding auctions that promote illegal activity. The auction was halted after eBay received a complaint from Microsoft. The listing[31] was posted by ‘fearwall’ who began the auction at U$0.01. He indicated that Microsoft was aware of the vulnerability and even offered to provide bidders from Microsoft with a 10% discount.

When discussing revenue and expenses for auction participants, we must discuss two separate parties - auction organizers and participants. For auction organizers, revenues are derived by retaining a percentage of the overall sale or charging a flat fee for the right to post an item for

[29] Greenemeier. *Unauthorized Patch For Microsoft WMF Bug Sparks Controversy*
[30] Lemos. *eBay pulls vulnerability auction*
[31] OSVDB Blog. *Selling Vulnerabilities: Going once…*

auction. Expenses would be driven by the costs necessary to establish and maintain the auction itself.

The greatest challenge facing a viable strategy for establishing an auction of private vulnerability research is the ability to communicate the value of the information without actually divulging the vulnerabilities. Unlike physical goods, information cannot be shown to a prospective buyer, and then withdrawn. Once it is known, the buyer no longer has incentive to pay for it. In the case of the Excel vulnerability discussed previously, the researcher attempted to overcome this by providing minimal details about the vulnerability. Without previously established relationships, it would be difficult to obtain full value from information when auctioning it in this manner.

2.5 Vendors

For the most part, vendors do not provide compensation for reports of vulnerabilities in their products. Historically, vulnerabilities have been freely and privately disclosed to vendors or disclosed in public forums without prior vendor notification. Until a few years ago, formal programs did not exist to compensate contributors; however, there are now a limited number of examples whereby compensation is provided. Despite the fact that most vendors do not pay for vulnerabilities, it would be difficult to argue that they do not benefit from having such information.

2.5.1 Compensation

Compensation can be made directly or indirectly. An example of direct compensation is the Mozilla Security Bug Bounty[32]. The Bug Bounty began in August 2004[33] and rewards those that report 'critical' security bugs with U$500 and a Mozilla t-shirt. While Mozilla is a California-based, non-profit corporation, initial funding for the project was provided by the private sector and Mozilla now accepts donations[34] in order to continue funding the program. Philanthropist Mark Shuttleworth, known for various endeavors including being a space tourist aboard the Soyuz spacecraft[35] matches all donations dollar for dollar up to $5000. The criticality of vulnerability submissions is determined by Mozilla, following guidelines posted on their website[36].

Microsoft does not pay researchers for vulnerability discoveries, but has established an Anti-Virus Reward program[37]. The program was established in November 2003 with an initial $5M investment and was designed to "help law enforcement agencies identify and bring to justice those who illegally release damaging worms, viruses and other types of malicious code on the Internet." Rewards of $250,000 have been offered for worms such as Blaster, SoBig and MyDoom, which took advantage of vulnerabilities in Microsoft technologies and resulted in widespread damage. While not a direct payment to security researchers, a correlation can be

[32] Mozilla Security Bug Bounty Program. http://www.mozilla.org/security/bug-bounty.html
[33] Mozilla Foundation. *Mozilla Foundation Announces Security Bug Bounty Program*
[34] Mozilla Donation Website. http://www.mozilla.org/foundation/donate.html
[35] Wikipedia. *Mark Shuttleworth*
[36] Mozilla Security Bug Bounty FAQ. http://www.mozilla.org/security/bug-bounty-faq.html#critical-bugs
[37] Microsoft Corp. *Microsoft Announces Anti-Virus Reward Program*

drawn to the Mozilla Security Bug Bounty in that this is a second example of a vendor paying unrelated third parties to improve the security or at least the perception of security in their products. This time however, the payment is not being made to reward researchers; rather it is being made to punish those that exploit previously discovered vulnerabilities.

While few vendors pay for vulnerability discoveries in the way that Mozilla does, it is not uncommon for software and hardware vendors to indirectly pay for original vulnerability research by way of security contests. The typical scenario involves a company exposing a fully patched and hardened device on the Internet and inviting the general public to bypass the security controls to achieve a particular goal. A prize is generally awarded to the first person to gain root access on the machine. There can be other motivations for running such a contest, such as the publicity that is generated as was the case for a proposed $1M hacking challenge proposed by Canadian hardware vendor AlphaShield[38]. Ultimately, companies clearly benefit from having a large pool of QA testers that are not on the payroll.

2.5.2 No Compensation

Most vendors do not compensate researchers that report vulnerabilities in their products. While they may provide alternate motivations, such as publicly thanking the researcher for their efforts, monetary compensation is not provided. Vendors clearly have different motivations for not launching bug bounty programs, but the arguments generally fall into the following categories:

- Altruistic – Some feel that researchers have a moral obligation to privately report security vulnerabilities to vendors.
- Status Quo – Historically, compensation has not been provided for vulnerabilities. Even with the emergence of third-party commercial programs, vendors continue to receive vulnerability reports without having to provide compensation.
- Competition – As vendor compensation programs are largely uncharted territory, there is often concern that providing compensation of any kind will create an undesirable marketplace in which vendors and third parties compete for information.
- Blackmail – Some fear that providing compensation of any kind will open vendors up to blackmail, as individuals will demand unrealistic sums in exchange for vulnerabilities. If the ransoms aren't paid, the vulnerabilities could be publicly disclosed or sold to third parties, possibly in the underground.

3 Impact/Implications

3.1 Government

The perceived value of private vulnerability knowledge for governments depends on the intended use of that vulnerability information. If the intended use is for the defense of existing systems, the perceived value for governments is similar to the perceived value for private companies. There is value in having knowledge of vulnerabilities ahead of the general public so that workarounds can be applied before patches become available. However, there is no value in

[38] Leyden. *$1m Hacking Contest Planned.*

withholding vulnerability details from the affected vendor, as an ‘official’ patch is generally deemed to be a better countermeasure than a temporary workaround.

If, however, vulnerability information is to be used for offensive purposes, then it is in the government's best interest to withhold details of the vulnerability from all affected parties including the vendor. If details were leaked, potential targets could protect themselves from attack. Beyond this, if the vendor were to learn of the vulnerability, they could issue a patch that would ultimately become widely available, greatly diminishing the value of the vulnerability for offensive purposes.

While having governments leverage financial resources to obtain vulnerability information might have national security benefits, those benefits come at a cost to all others using the vulnerable technology. When vulnerabilities are used for offensive purposes, it is always in the government's best interest to suppress such information for as long as possible.

3.2 Open Market

The Open Market and Internal Discovery models can have a large impact on the nature of security, especially with regard to how vulnerabilities are discovered and addressed. Additionally, there are important implications that result from the widespread implementation of these models. Perhaps the most important impact is the ability of these models to uncover vulnerabilities that may have been known in the underground for some time and the ability to increase the focus on vulnerability discovery within the industry. The important implications include the potential for information leaks from within a company following one of these models, and the fact that large customers that can afford the advanced knowledge and protection services will be protected before vendor patches are available while the rest of the Internet society will not.

Open Market models help to bring issues known to the underground to the vendors' attention, benefiting the Internet society as a whole. More specifically, the Open Market models implemented by iDefense and TippingPoint help to draw out vulnerabilities that are known in the underground community. If a vulnerability researcher, or anyone involved in the underground community for that matter, uncovers a known vulnerability that has not been fixed, they could sell it to iDefense or TippingPoint. This person would be paid, and once the issue was fixed, the Internet society would be safer. The Open Market model also focuses on vulnerability research within the information security industry. The Outsourcing and Internal Discovery models encourage and fund the efforts of vulnerability researchers. As more vendors accept the need to work with these researchers to improve the security of their products, Internet security as a whole will improve. Additionally as more Outsourcing and Internal Discovery models prove to be profitable, more companies will enter this space, resulting in an increased focus on vulnerability research.

The most obvious potential consequence of the Open Market model is that somewhere within one of the companies implementing the model, there will be a leak. The companies are able to say that they deal with vulnerability information in an ethical way because they report the information only to their clients and the vendor. However, if an employee or client leaks details

about the vulnerability to the public or the underground before the vulnerability is fixed by the vendor, there could be serious consequences. To protect against this, companies employing these models must have non-disclosure agreements in place with both employees and clients that threaten legal action if the agreement is broken. While NDA's cannot guarantee there will be no leaks, they can significantly discourage individuals from leaking vulnerability information.

Another important implication of the Open Market model is that only companies and individuals that can afford these services will be protected in advance. All other parties must wait until the vendor issues a patch, which can take months or years, making this model more beneficial to the Federally Funded Social Planner suggested by Kannan et. al.[39] than to society as a whole. In most situations, those who can afford the products offered via this model have more valuable assets to protect and are more willing to spend the required funding to purchase these products.

3.3 Underground

Due to the discrete nature of the underground market, it is hard to precisely gauge this model's impact and implications. However, extrapolating on known information allows us to determine some of the successes of the underground models. Were these models to gain momentum, the result would be that vulnerability details would be suppressed and numerous vulnerabilities would go unpatched for extended periods. The most apparent implication is that if these models successfully generated revenue, they would be used more often. Success of the underground contracted and purchased models would mean that vulnerability researchers would have less incentive to report vulnerabilities directly to vendors and not get paid or to go through third parties such as iDefense or TippingPoint that would pay for the research. Both of these routes lead to the vulnerability being fixed, and once patches are widely deployed, the exploits become less valuable. However, if the vulnerability remains unpatched, the vulnerability researcher can continue to sell the same exploit to multiple parties. Had use of the WMF exploit gone unnoticed for a longer period of time, the discoverer of that vulnerability could have profited even further. The more successful and widely implemented these models are, the less often details of vulnerabilities reach the vendors who can properly fix them. Additionally, over time, the success of these models will continue to grow and gain momentum. Knowing that the discoverer of the WMF vulnerability made $4,000 USD each time an exploit was sold, and assuming that the $10,000 USD prize from iDefense for reporting a critical vulnerability in a Microsoft product is on the high end of the pay scale for iDefense and TippingPoint, then a vulnerability researcher who found such a vulnerability would realize that they need only sell the exploit on the underground to three malicious actors to make more money than they could by reporting it to the vendor via a paying third party. Additionally, the same vulnerability researcher need only sell the exploit to one malicious actor to make more money than if they reported it directly to the vendor. Therefore, as the feasibility of the underground models increases, more and more vulnerability researchers will realize that they can make more money by not going public with the vulnerability.

3.4 Auction

[39] Kannan, Telang, Xu. *Economic Analysis of the Market for Software Vulnerability Disclosure.*

As discussed, vulnerability auctions face a fundamental challenge that has thus far prevented viable auction models from emerging. Until an auction strategy is devised that allows potential buyers to assess the value of the vulnerability without disclosing full details, auctions are unlikely to emerge as a viable economic model. The establishment of trusted escrow agents would be one potential solution to this problem.

The Auction model shares the same overall drawback as the Government model. The entity purchasing the vulnerability is presumably doing so as the information is of greatest value so long as it remains private. This in turn places users of the vulnerable technology at risk because the vendor is unaware of the vulnerability and cannot produce a patch.

3.5 Vendors

Today, only a select few vendors directly or indirectly pay for vulnerability information. In all of the economic models researched for this paper, it is clear that vulnerability information has value to the parties seeking to obtain it. This certainly holds true for vendors. The presence of vulnerabilities has the potential to negatively impact affected vendors financially. If clients lose confidence in a vendor's ability to produce secure technology, the damage done to a vendor's corporate reputation can be translated into lost sales. It is for this very reason that Microsoft has spent billions of dollars to launch their Trustworthy Computing Initiative[40].

Interestingly, of all of the economic models researched, the Vendor model is the only one in which interested parties receive the benefit of vulnerability information without paying for it. Many feel that it is a necessary component of responsible disclosure for researchers to report vulnerabilities directly to vendors without compensation. However, as this is not a legal requirement, in a free market enterprise it is not surprising that a number of economic models are emerging to profit from vulnerability information. If vendors maintain a policy of not paying for vulnerability information, it is likely that over time, fewer researchers will be willing to report vulnerabilities directly to vendors as economic incentives continue to arise elsewhere. Vendors have the power to reverse this trend, but only if they are willing to pay for research from which they already benefit.

As consumers become more knowledgeable about the risks posed by vulnerabilities, vendors have been forced to change their behavior. Today, most vendors have a process in place to allow third parties to report vulnerabilities as they are discovered. Without economic incentives for reporting vulnerabilities directly to vendors, it is imperative that the process be simple and straight forward. Some vendors opt for a basic reporting mechanism such as publicizing a specific e-mail address (e.g., security@vendor.com) that is to be used for such reports. Others use online web forms to better structure the reports that are received. Larger vendors have also dedicated significant manpower to respond to reported issues and ensure that they are addressed in a timely fashion. Microsoft, for example, has established the Microsoft Security Response Center (MSRC). MSRC acts as a middleman between researchers and developers. They perform triage on incoming reports to identify those that are legitimate, then work with developers to ensure that patches are produced and pushed to clients.

[40] Lemos. *One year on, is Microsoft 'trustworthy'?*

Vendors are also making efforts to work more closely with researchers to encourage them to report vulnerabilities. Today, many vendors credit researchers when issuing security advisories as a means of publicly thanking them for responsibly reporting the issue. Others, even proactively seek to build relationships with the same researchers that uncover vulnerabilities in their products. Microsoft for example, throws a lavish party each year at the BlackHat security conference in Las Vegas, NV. They also hold an internal security conference known as BlueHat, where researchers are flown to Microsoft's Redmond headquarters to teach Microsoft developers how they were able to break their code. Initiatives such as these may seem excessive to some, but are vital when researchers already have strong economic incentives to go elsewhere with their findings.

4 Conclusion

While, many will debate the ethics surrounding the commercialization of vulnerability research, it is difficult to deny that vulnerabilities have value. The numerous economic models discussed in this report serve as evidence of that fact.

As the world places more data online and becomes increasingly reliant on computer systems, governments will become more interested in obtaining private vulnerabilities, facing increased competition from the commercial sector to obtain the necessary human resources to develop this intelligence. As a result, governments must invest in training programs to develop talent in-house and further contracting initiatives to obtain talent from the private sector.

The open market will continue to grow as companies become more aware of the risks faced by exposure to vulnerabilities and look for a means to be protected as early as possible.

We are seeing more signs of the underground's profit motive. Spam, spyware, adware and phishing attacks, while largely illegal, are fueled by the money they can generate. It is clear that such attacks are no longer simply the work of misguided individuals, they are now well orchestrated attacks funded by organized crime. Given the profit potential in the underground, we can expect this market to grow.

The emergence of auctions is less clear. In order for auctions to be viable, trusted escrow agents that can validate the value of vulnerabilities offered for sale must be established. While there is evidence of such agents emerging in the underground at websites such as http://web-hack.ru/, given the controversial nature of selling vulnerabilities, it is unlikely that a trusted corporation would be willing to fill this role. It is expected, therefore, that auctions will not emerge as a significant market for trading vulnerabilities.

As government, open and underground markets continue to grow, vendors will be forced to reassess the policy of not paying researchers for vulnerability research. It has been established that vendors benefit financially from such information, so their decision to not pay researchers seems to be driven by attitudes and perceptions of the practice as opposed to economic factors. From an economic perspective, the traditional vulnerability market whereby vendors receive the benefit of vulnerability data without paying for it is the only model whereby offsetting expenses

and revenues do not push the market to a state of equilibrium. If vendors do not change their stance on this issue, the percentage of overall vulnerability information provided exclusively to them will diminish over time.

Bibliography

Billo, Charles G., Welton Chang. *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States.* Dartmouth College. Nov. 2004. http://www.ists.dartmouth.edu/directors-office/cyberwarfare.pdf.

Bohme, Rainer. *Vulnerability Markets: What is the economic value of a zero-day exploit?* 22nd Chaos Communications Congress. Dec. 28, 2005. http://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf.

Defense Science Board. Protecting the Homeland: Report of the Defense Science Board Task Force on Defensive Information Operations 2000 Summer Study Volume II. United States Department of Defense. Mar. 2001. http://www.iwar.org.uk/iwar/resources/dio/dio.pdf.

Endler, David. *Announcing the Zero Day Initiative.* Dailydave Mailing List. July 25, 2005. http://seclists.org/lists/dailydave/2005/Jul-Sep/0102.html.

Evers, Joris. *Offering a bounty for security bugs.* CNET News.com. July 24, 2005. http://news.com.com/Offering+a+bounty+for+security+bugs/2100-7350_3-5802411.html.

Gonsalves, Antone. *Microsoft Slams Security Firm's Bounty For Windows Flaws.* InformationWeek Magazine. Feb. 21, 2006. http://www.informationweek.com/news/showArticle.jhtml?articleID=180205623.

Greenemeier, Larry. *Unauthorized Patch For Microsoft WMF Bug Sparks Controversy.* InformationWeek Magazine. Jan. 4, 2006. http://www.informationweek.com/software/showArticle.jhtml?articleID=175801150.

House Select Committee on Homeland Security: Subcommittee on Cybersecurity, Science and Research & Development. *Hearing on Putting the "R" back into "R&D": The Importance of Research in Cybersecurity and What More Our Country Needs To Do.* United States House of Representatives. July 22, 2003. http://www.cs.columbia.edu/~smb/papers/transcripts_cybersec_072203.htm

Kannan, Karthik, Rahul Telang, Hao Xu. *Economic Analysis of the Market for Software Vulnerability Disclosure.* 37th Hawaii International Conference on System Sciences. Oct. 1, 2003. http://csdl2.computer.org/comp/proceedings/hicss/2004/2056/07/205670180a.pdf.

Keizer, Gregg. *Firm Offers $10K Reward For Critical Windows Bug.* InformationWeek Magazine. Feb. 17, 2006. http://www.informationweek.com/windows/showArticle.jhtml?articleID=180204079.

Lemos, Robert. *eBay pulls vulnerability auction.* SecurityFocus. Dec. 9, 2005. http://www.securityfocus.com/news/11363.

Lemos, Robert. *One year on, is Microsoft 'trustworthy'?* CNET News.com. Jan. 16, 2003. http://news.com.com/2100-1001-981015.html

Leyden, John. *$1m hacking contest planned.* The Register. May 1, 2001. http://www.theregister.co.uk/2001/05/01/1m_hacking_contest_planned.

Mark Shuttleworth. Wikipedia entry. http://en.wikipedia.org/wiki/Mark_Shuttleworth

Microsoft Announces Anti-Virus Reward Program. Microsoft Corp. Nov. 5, 2003. http://www.microsoft.com/presspass/press/2003/nov03/11-05AntiVirusRewardsPR.mspx

Microsoft Security Bulletin MS06-001. Microsoft Corp. Jan. 5, 2006. http://www.microsoft.com/technet/security/Bulletin/ms06-001.mspx.

Mozilla Foundation Announces Security Bug Bounty Program. Mozilla Foundation. Aug. 2, 2004. http://www.mozilla.org/press/mozilla-2004-08-02.html

Naraine, Ryan. *Researcher: WMF Exploit Sold Underground for $4,000.* eWeek Magazine. Feb. 2, 2006. http://www.eweek.com/article2/0,1895,1918198,00.asp.

National Technical Information Service (NTIS). Report of the Defense Science Board Task Force on Defensive Information Operations, Volume II-Part 2, Annex G. *The Cyber Operations Readiness Triad (CORT).* June 2001. http://cryptome.sabotage.org/nsa-cort.htm.

Nizovstev, Dmitri, Marie Thursby. *Economic Analysis of Incentives to Disclose Software Vulnerabilities.* Workshop on the Economics of Information Security 2005. June 3, 2005. http://infosecon.net/workshop/pdf/20.pdf.

Ozment, Andy. Bug Auctions: *Vulnerability Markets Reconsidered.* Workshop on the Economics of Information Security 2004. May 13, 2004. http://www.dtc.umn.edu/weis2004/ozment.pdf.

Selling Vulnerabilities: Going once... OSVDB Blog. Dec. 8, 2005. http://www.osvdb.org/blog/?p=71.