Vulnerability Black Markets: Empirical Evidence and Scenario Simulation

Jaziar Radianti
University of Agder
Serviceboks 509
4898 Grimstad-Norway
jaziar.radianti@uia.no

Eliot Rich
School of Business
University at Albany,
State University of New York
e.rich@albany.edu

Jose. J. Gonzalez
University of Agder
Serviceboks 509
4898 Grimstad-Norway
jose.j.gonzalez@uia.no

Abstract

This paper discusses the manifest characteristics of online Vulnerability Black Markets (VBM), insider actors, interactions and mechanisms, obtained from masked observation. Because VBM transactions are hidden from general view, we trace their precursors as secondary evidence of their development and activity. More general attributes of VBMs and the exploits they discuss are identified. Finally, we introduce a simulation model that captures how vulnerability discoveries may be placed in a dual legal-black market context. We perform simulations and find that if legal markets expose vulnerabilities that go unresolved, the security and quality of software may suffer more than in the absence of a legal market. Thus the problem scope expands beyond vulnerability trading to one that requires active participation and reaction by software vendors.

Key words: black markets, masked observation, system dynamics, software vulnerability, simulation

1. Introduction

Software vulnerabilities are one major root of today's computer security problems [1]. These vulnerabilities are accessible by skilled and novice infiltrators enabled by rootkits, scripting tools and other easily disseminated tools. Exploitation of security holes for commercial gain or sabotage creates the opportunity for black markets (BMs) where vulnerabilities are solicited and traded.

The vulnerabilities and exploits circulated in the underground are already subject to public discussion and prominent in several well-known security companies' reports, for example X-Force Report from IBM [2], PandaLabs [3], Symantec [4] and Finjan [5].

The term "Black Market" originally appeared in the economic literature during the Second World War, when rationing in the United States was coupled with price ceilings for many major consumer commodities [6]. BMs are "black" as they support illegal activities occurring under conditions of great secrecy [6, p. 2]. More recently, the term Vulnerability Black Market (VBM) is used to describe illicit trading of software vulnerability information over the Internet.

In previous work [7], we have used system dynamics (SD) models to portray the problem and simulate consequences of a VBM for software vulnerabilities. The nature of the VBMs is elusive and good data is scarce. An open observation of VBMs is hardly possible. Hence, we performed a masked observation of online VBM forum activities, which we describe below.

The purpose of this paper is to provide some eye-opening information and discuss the VBMs issue in connection with software security problems. We target several objectives: first, to assess the empirical evidence for VBMs; second, to derive more general attributes of the black market for vulnerabilities and exploits from our observations; third, using a concept model to qualitatively assess if a vulnerability legal market would improve vulnerability disclosure. We organize the paper into six sections: Introduction, Theory of Vulnerability Black Markets, Data: Method, Source and Procedures, Results, Concept Model, and Conclusion.

2. Theory of Vulnerability Black Markets

Literature related to the trading of software vulnerabilities is very limited, but may be categorized into three types. *First,* there are theoretical works on the economics of information security. Authors assume that black markets for vulnerabilities exist and focus on the mechanisms needed for a parallel legal market, such as pricing and market failures. *Second*, additional theoretical works on vulnerability market models have been derived from expert observation and experience. *Third*, recent literature infers the existence of VBM behaviors based on empirical examination of such markets. These works

978-0-7695-3450-3/09 $25.00 © 2009 IEEE

attempt to capture and explicate the nature, mechanism and actors, and ultimately, estimate the security threat presented by VBMs.

Ozment's [8] and Böhme's [9] works are examples of the first type. Ozment proposes an auction model for vulnerability markets and assumes that VBMs exist and may offer great rewards to hackers. In his view, the use of direct rewards for vulnerabilities will open the door for arbitrage. He discusses the use of a Dutch auction model, where sellers expose their goods for sale with an initial offering price that can only be lowered, ensuring that vulnerabilities are reported immediately. A downside of such a market structure is the possible attack on bidders or their agents.

Ozment (ibid) claims that the resale of vulnerabilities is particularly troubling. Resale occurs when in-house or outsourced software testers sell vulnerability reports to third-party or malicious hackers. This is a special type of double-dipping peculiar to information-based commodities, as the testers have the opportunity to expose manifest problems to hackers before developers can patch them. Buyers of these vulnerabilities would then acquire a short-lived commodity, reducing their confidence in the process for future transactions. Ozment concludes that there are few solutions to this dilemma; but he is optimistic that having auctions for vulnerabilities would reduce the incentives for resale.

Böhme [9] also advocates the development of an auction strategy, where "an adversary would have an incentive to report the bug instead of exploiting it or selling it on the black market." These works offer some insight into the use of formal vulnerability markets to improve software quality.

Miller's [10], and Sutton and Nagle's [11] works belong to the second type, as they are grounded in observation rather than theory alone. Miller, for example, notes that BMs for computer exploits provide alternatives for security researchers to sell vulnerability information. Claims about spammers and criminals' accessibility to zero-day exploits as well as speculation about the VBM price are based on several internet sources.

Sutton and Nagle [11] present another picture of economic models for underground vulnerabilities, focusing on their revenue stream. They propose two constructs, the *contracted model* and the *purchase model,* to explain underground operations. In the contracted model, a malicious actor hires a hacker to find vulnerabilities in specific software targets. The vulnerability, if part of widely deployed tools, could be used to "power spam," attach spyware or insert adware. If the contract was targeted at a firm, illegal revenues could come from espionage or blackmail. The authors called this phenomenon a "hacker-for-hire" industry. They point out the possible contacts between vulnerability sellers and buyers through underground websites and Internet Relay Chat (IRC) rooms. In some sites, malicious actors can even post the vulnerabilities for which they are looking, allowing hackers to review and decide whether they want to take the job. The authors support this argument by pointing out a web-hack site, allegedly a site for underground activities.

The purchase model reverses the contracted model. Here, the hacker finds a vulnerability, creates an exploit and sells it to the malicious actors. The authors emphasize that all parties have to broker the deal, involving some potentially risky contracts, while making sure that they are not caught by law enforcement. Naraine [12, 13] reports on a purchase model transaction, where the Microsoft Windows WMF vulnerability was discovered and sold on the underground market to malicious actors.

Security companies have created their own vulnerability marketplaces. An example is the Zero Day Initiative (ZDI) launched by TippingPoint [14]. This program proposes to pay researchers for data on vulnerabilities, acting as a broker between market actors. The company promotes *responsible disclosure* by working closely with affected vendors to get patches to market quickly. This approach also counters concerns that security researchers are not properly compensated and are driven to the dark side [15]. Researchers may prefer not to deal directly with vendors, and a brokered market can prevent resale of vulnerability information to malicious agents [16]. The opportunity for a trusted market decreases the chance that vulnerability research will be marginalized and moved further underground. This, in turn, would create longer windows of consumer exposure to potential threats.

In recent years, other researchers have found empirical evidence of vulnerability markets to complement the theoretical research. We found several Internet black market-related studies, notably Franklin et al. [17] and Zhuge [18]. The former relies on IRC networks to collect market data. The latter uses automated browser technique on the visible web to identify websites with malicious contents. These works take a broader and more systematic approach towards establishing an empirical base for VBM observation.

Franklin et al. [17] study underground activities using a dataset collected over 7 months and comprising 13 million messages over IRC channels. In their work, they record illicit market discussions and solicitations. This dataset categorizes the participants, exploits and the good and service offered. Franklin et al.'s study focuses on sensitive data trading, such as secret information related to credit cards. The study included no discussion of tools, malware or other vulnerability exploits.

Captivatingly, Franklin et al. [17] propose direct interference with these channels as a countermeasure to interrupt BMs. Traditional law enforcement approaches

are costly and the legal infrastructure surrounding software vulnerabilities is poorly developed. Sites often disappear and re-emerge under a stronger hosting infrastructure. This study proposes two techniques to turn the anonymity of the Internet back on the black hat community. The first is the use of a *sybil attack,* creating multiple identities, destabilizing participant verification, and creating a "market for lemons" [19] among buyer and seller. The second counter-measure they discuss is a *slander attack,* to blacken the reputation of other participants through false defamation. Both aim at creating distrust environment among participants and reducing the opportunity for successful transaction. The hoped-for outcome is the exit of participants from the IRC channel and the vulnerability markets.

Zhuge et. al [18] evaluate about 145,000 of the most commonly visited websites on the Chinese web and found that 2,149 contained malicious content. They also perform redirection link analysis which can disclose the relationship between malicious websites and the hosts of web-based exploits. Their study provides additional information about the parallel structure of the dual nature of visible and underground aspects of the problem.

Our previous study [20] proposes other possible methods to approach and explain this market. Although we have not yet presented a final result, we have already noticed similar characteristics of VBMs. Below we discuss how we examine the interaction between the individual actors within the market, the market mechanism, various advertisements in the forum, and scrutinization of types of virtual goods that may abuse the software vulnerabilities with malicious intention. This work allows us to create hypotheses about patterns of VBM activities over time.

3. Data: Method, Source, and Procedures

***Source*:** Our sources to explore online VBMs come from various "underground" websites. We begin our investigation on VBM existence through a link referred by a security news article as a place to conduct online illegal activities. Through this process we are able to discover more forums, since directly or indirectly, some active participants cite, refer or even invite others to visit their forum.

Method: Once a site was identified, we would visit it and observe the activities related to zero-day exploit and other vulnerability-related attack tools. Observation is recommended by Luna-Reyes and Andersen [21] as one of several qualitative social methods that may contribute to developing a SD model. In this research mode, quiet observation without participation is a viable technique for data capture without interfering with the actors.

VBM sites often use message boards and Internet Relay Chat networks. Both of these tools are usually accessible to visitors. Occasionally, the VBM's message boards require registration with a valid email address in enrollment. More restrictive forums stipulate certain requirements to establish poster credibility, such as minimum posting activity level, before entry to the VBM forum is permitted. During this study we registered on boards with an anonymous email address, disguising our identity so that we could explore all message board areas.

We observed 12 VBM forums shown in Table 1 coded as W1…W12, which we roughly categorize as small forums (website with less than 15,000 members) and large forums (website with more than 15,000 participants). We argue that this differentiation is helpful to understand the sustainability of the VBMs. Participants appear to prefer large forums where the number of potential buyers is high, and leave unpopular, small ones.

Table 1
Observed Forums and No. of Threads

Code	No. of Threads (as of)	Earliest Post in	Forum Name
W1	849 (May 2008)	2006-04-20	Black Market
W2	1251 (May 2008)	2007-06-18	Marketplace
W3	16 (May 2008)	2006-12-13	Advertise
W3a	N/A	N/A	Only IRC
W3b	46 (May 2008)	2007-11-30	Black Market
W4	*Used to have BM Forum, now unavailable*		
W5	82 (N/a)	N/A	*Forum down*
W6	655 (May 2008)	2007-02-24	Buy-Sell-Trade
W7	5 (May 2008)	2007-10-31	Black Market
W8	17 (May 2008)	2006-07-14	Money
W9	10 (May 2008)	2006-05-03	Vulnerability
W10	2 (May 2008)	2007-10-10	Black Market
W11	18 (May 2008)	2007-12-02	Black Market
W12	27 (May 2008)	2007-12-29	Trade Center

In both small and large forums we found that the three criteria for a potentially viable VBM were met. We observed the presence of buyers and sellers, identified mechanisms for them to meet, and noted a viable medium of exchange. Some websites changed their hosting country, perhaps as a mechanism to remain secure. Others disappeared and re-appeared, reborn or split as new forums. Some closed before we were able to capture data. VBM websites may contain VIP sections, with elevated requirements for posting activity, participant recommendation, exploit sharing tools and monthly fees. Our research was limited to sites where we could observe without contributing or soliciting exploits. We believe that there are more online secretive VBM sites beyond those 12 forums which remain hidden from public view, because we found 5 new VBM forums established in April-May 2008. Zhuge et. al's study found 2,149 malicious websites in China alone, although there was no

explicit clarification of whether these malicious websites contained BMs.

Procedures: *First,* we explored all topics and advertisements in each forum and thread of activity. The text was recorded and dated. Coded archives were developed to track the each activity and conversation thread. *Second*, we coded crucial and relevant characteristics in a cases-attributes matrix. Attributes included:

- title of thread,
- name of thread originators,
- join date and posting date,
- membership status in the forum,
- intention to open the thread
- contact method(s)
- payment method(s) and price (if available)
- offered tool's specification

Special notice was taken of unique discussions and distinctive cases. The bulletin board structure allowed participants to immediately reply on the same thread. Therefore we could follow development of the discussion.

Our goal for this effort was two-fold. First, we wanted to collect information on the types of activities that occur on public and semi-public sites purporting to support hacking activities. Second, we wanted to examine how site activities develop over time so that we could form testable hypotheses of the mechanisms and growth of black markets.

4. Results

Basic Traits of VBMs: We reflect upon a number of characteristics of the observed VBM forum, and in some ways differentiate between large and small forums:

First, all forums carefully avoid excessive visibility and disappear intermittently for some weeks. In some cases, the problem is purported to be technical, such as server crashes and lost databases. In other situations, the forums are themselves victimized through a D-DoS attack. Sometimes the hosting organization cancels the forum as malicious content or activity becomes apparent. A final reason for intermittent activity occurs when the forum leaders argue or want to purge the site of registrants with invalid addresses or no postings. Not surprisingly, to avoid D-DoS attack, certain forums will redirect visitors to another URL.

- *Second*, as a forum grows the administrators enact increasingly strict rules limiting and controlling the VBM activities and participant growth. For example, forums may institute minimal posting levels for continued membership. They also regulate prohibited traded goods. Two public mechanisms for controlling behavior are seen. Threads that contain rule-breaking postings are locked. Offending posters are often provided multiple warnings before being banned from the site. Smaller and emerging forums seem to have fewer restrictions. This may imply less monitoring of the board by its owners, or a laissez-faire approach that enables growth towards a desired state. *Third*, each forum has membership levels, from newcomer or newbie to the higher rank. The administrator and moderators are typically in the highest level. We identified the rank from the member information label appearing next to a post. The particular ranks and names vary among sites, but the ordinal sequence is clear. In addition, there is often a "Banned" member category.
- *Fourth*, members use nicknames rather than real names. They often use e-mail domains that are recognized as forwarding sites. In many cases, the given age and geographical location is obviously wrong. This obscurity indicates that participants want to be anonymous.
- *Fifth*, nearly all forums have rules and social norms. There are few formal rules to trade in VBMs, with uneven rule emphasis, strictness and consistency across forums. Many rules are unwritten, but every player understands them. Examples of common written rules include reinforcement of behaviors: limits on flaming and reminders not to scam others. The participants must be willing to provide verifiable email accounts. There are often limits on explicit discussion of clearly illegal activities, such as credit card or bank logins, botnets or hacking requests; such requests are often diverted to private messages or chats, the true back alleys of the Internet. As noted earlier, we found that there are often minimum posts to enter the VBM section of the site. Other rules include reminders about the risks of malicious or D-Dos attacks. These rules enact some of the obvious actions proposed in the academic literature that would force the closure of the site or loss of reputation.
- *Sixth:* There is no righteousness among online VBM burglars. The terms such as "ripper", "leaker" or "scammer" are quite popular among underground actors. A ripper is considered as a serious outrage in VBMs; it describes a buyer who violates the agreement by taking the malicious tools without paying the seller; or a seller who cheats the potential buyer by accepting their payment without delivering the virtual goods in return. Such behavior has a serious impact on the buyer's or seller's reputation, because members distrust sellers or buyers with blemished records.

Actors in VBM: The structure of these sites is relatively consistent, owing in part to the features of the

underlying technology. We found that there is often a clear hierarchy of actors.

Webmaster, administrators and moderators work together to monitor and mediate all discussions occur in message board area. This is an important task within in the VBM forum, as these actors have a vested interest in maintaining the service. The administrator regulates the size of the market by adding basic requirements for new participants that want to advertise materials. They may also attempt to verify the quality of postings by reviewing the legitimacy of the posters and their wares. In some forums, administrators choose to edit postings containing inappropriate and abusive comments. Moreover, the webmaster, administrators and moderators from each forum have particular ideas about their role in the market process. Their views and perceptions are reflected from the rule or comments in their postings. From Zhuge's study [18], we learn that in some underground websites, the webmaster may act as an intermediary who attracts visitors' attention by providing free music or film downloads. Conversely, the actual motive for having many visitors is to develop and sell website visit logs to *Envelope Stealers*. Thus, it seems there are two interests that a webmaster should safeguard: to attract visitors and regulate "access" for participants in certain "restricted" forum such as VBM.

Active sellers are identified in the forums by their postings. They may be individuals who use their technical skills to investigate and find the weaknesses in software. They may also write scripts for exploits and develop malware that could take advantage of discovered problems. Observed sellers include:

- *Spammers,* who extend existing spam-related tools, such as mailers, spreaders, email addresses, logins and passwords.
- *Exploiters,* who offer various zero-day exploits to gain access to computer administrators, or collect victim computers that can be used to host a phishing site or a spam transmission.
- *Carders,* who actively offer various CC and CVV2, to create various fake CC. However, most observed VBMs reject participants advertising CC-related or online banking accounts and logins.
- *Virus / Malware Writers,* who look for vulnerabilities in software and develop exploits. Some exploits may be developed from scratch, while others are modifications from previously available exploits or malware. They are also able to code certain "obfuscator" tools to hide malicious files from anti-virus tools.
- *Hosting owners* who offer a site for hosting scam pages
- *Cash out for hire*: a person who offers a service to cash out a certain financial account.
- *Coder, hacker for hire*: a participant who offer their technical knowledge in coding to develop specific tools or to hack specific sites.

Active buyers may also be identified from the intention of their postings:

- *Script Kiddies,* participants who want to exploit computers without having high skill, look for "ready-made" kits malware or exploits in VBMs.
- *Spammers* can also be found as buyers.
- *Service Requests* come from individuals looking for others to hack, create exploits, to make their malicious files undetected by most anti-virus software or to code malicious tools.
- *Card buyers* are the counterparts of carders; they search for carders. Most forums reject both carders and card buyers by locking the communication when they are detected.

There is also a type of buyer who does not directly announce the nature of their request. Instead, they respond to a posting by asking for access to a private communication channel.

Active Participants are much more difficult to identify as they may only make comments without a clear indication of whether they intend to sell or buy. However, some of them may be experienced hackers and their comments are sometimes quite critical, affecting the market in terms of trust and reputation.

Lurkers are participants who may visit VBM forums without active involvement in any activities or discussions.

Contact: Communication via the Internet makes the user's real identity untraceable through observation. Popular contact methods include forum-based private messaging, instant messaging, and alias e-mail addresses. In our sample, private messaging is most often employed. In the absence of third-party encryption, though, these messages may be visible to the board administrators. Instant messaging, using the facilities of Yahoo Messenger, AIM, MSN, ICQ and IRC, are also popular. These tools provide a way for sellers and buyers to reach each other outside the board and on their own schedule. Some participants accept email communication. Free email accounts such as *Hotmail, Yahoo*, and *Gmail* are commonly employed. As message boards often have internal mechanisms for private messages, we assume that this approach is popular, though not visible to persons outside the domain.

Transaction: Payment Methods and Pricing: The obscurity and secrecy of VBM trading carries over to payment methods. The use of online money transfer seems more attractive than the traditional paper methods such as cheques and money orders. The most popular payment methods are *e-gold* (www-e-gold.com) providing gold conversion services and *webmoney* (www.wmtransfer.com), providing seven types of electronic currency in circulation across various websites. Within these realms our NM participants prefer WMZ, a currency linked to USD. Other currencies or mechanisms include *ePassporte*, *PayPal*, *Moneybookers*, *Money Gram*

and *Western Union (WU)*. Within German-based sites, the PSC (Paysafecard) seems popular.

All the services purport to validate and send payments instantly. In this realm, actors are caught in a dilemma, where they want to ensure the completion of their transaction but also avoid tracing and detection. The message boards themselves sometimes contain discussions on the relative merits of payment schemes. We find there are many different payment services in play. Each financial service has slightly different requirements for their users. Some services permit people to transfer money after providing only an e-mail address. E-gold's relatively high fees and processing steps can discourage some users. Others reject PayPal because of a belief that it is insecure and, ironically, because it is a frequent target for hackers. There are some limits on service availability in different areas. Usually payments are not recoverable – *caveat emptor*.

E-gold's management recently pled guilty to charges of money laundering and conspiracy to operate an unlicensed money transmitting business in the US courts [22]. As part of their plea agreement, e-gold's management agreed to amend their services and procedures and increase individual accountability for transactions. Their service is still available, although BM participants apparently possess multiple alternatives money transfer methods for their illegal virtual business.

Few participants discuss pricing in plain language; perhaps participants prefer private messaging or a non-public room to discuss the transaction. A few members use flexible methods by accepting three or four different payment methods; depending on the consumers' demand. We also found cases where sellers or buyers propose an *escrow* service, where exploits and funds are held by a third party until the fulfillment of various conditions.

Previous researchers have reported rather extreme seller-side prices for exploits. These reports include a $50,000 Vista flaw (from a Romanian web forum) [13], a WMF exploit for $4,000 [12], and other zero-day attacks, ranging from $5,000 and $20,000 [13]. Other solicitations include offers for a 'weaponized' exploit in for $20,000 to $30,000 [23] and zero-day vulnerabilities on the Internet black market for $25,000 [24].

Our own observations find that these prices are rarely reached. It is almost impossible to find any offer in observed VBMs in these ranges. Table 2 provides a selected price quotation we observed in the VBM. These do not represent the final price, of course, as we cannot see the transactions at market. The market participants appear to recognize appropriate price ranges based on the type of product and how it is developed (i.e., custom work or modification of an existing exploit). One interesting conversation between actors revolved around a low-cost offer for an IE6 or IE7 exploit. A potential seller criticized the offer noting that legitimate markets such as iDefense would pay much more than he is willing to pay for such bugs. This gives some indication that the availability of a legal market presence provides some bargaining power to sellers.

Table 2
Examples of Some Prices of Traded Goods

Product Type	Cost
Packers-Related	$ 50 - 100
Some exploits	$ 500 – 1,000
MPack Exploit bidding	Start from $ 150
Shop Admin Exploit	$ 100 – 300
Mass mailing	€ 50 – 70 / server
Undetected Obfuscators	$ 80
Full admin access	$ 300

Source: Observation in hacker websites, 2008

Traded Tools: Some of the exploit tools that are currently being traded include:

- *Bot tools* that develop and operate automated attacks on networked computers. The advertisements in VBMs include executables, source code, and particular bot flavors, including spammers, mailers and D-Dos attacks.
- *Remote Control* tools such as Poison Ivy (a kind of malicious trojan firewall-bypassing remote administration), Virtual Network Computing (VNC), a remote control software which allow users to view and interact with other computers over the network, and bifrost, a backdoor type and an advance remote administration tool that allow attackers to remotely control computers behind firewalls and routers.
- *Application Exploits*, such as for various web browsers, and shop administrators.
- *Hosting* and domain name services for hackers.
- *Packer-related tools* that hide the contents of malware, including crypter, binder, scramble, and obfuscator.
- *Financial information*, including credit card numbers and CVV2 numbers, bank accounts, logins and passwords, and PayPal and e-gold accounts.
- *Spam* tools such as email addresses, php-mailers, and mass-mailer tools.
- *System Administration* accounts such as root or administrative access to specific servers and admin logins.
- *Rootkit*s, tools used to maintain and mask root-level intrusions.
- *Password-stealing tools* with various name such as trojan grabber, bruteforce, keyloggers, password stealer, password grabber, password scanner.

Our findings differ somewhat from Franklin et al.'s results [17]. Their sample saw significant activity surrounding stolen data, such as credit card and CVV2 information. They also found notices of machines that have been compromised and are available for mass

mailings, electronic funds transfer fraud and phishing attacks. In our case, our larger black market sites rejected explicit sensitive data trading. When carders attempted to post, administrators often locked the threads before a public dialog ensued. There is no way to know if the transaction was completed.

There are many gray areas in this work, as licit and illicit activities can occur in the same location. One of our cases has VBM-related threads, targeting Microsoft products. The same site contains discussions of legal market practices among security researchers. Thus we note that sites perform legitimate roles for discussion and less savory roles hosting hackers and tools. This ambiguity of purpose is consistent with observations in the security literature that hackers are not easily classified as good or bad, and suggest that mechanisms might exist to encourage hacking to improve software quality rather than for attack. We build on this idea to develop a simulation of such a mechanism.

5. Concept Model

In this section we present a "concept model" derived from our recent understanding about the features of a black market for vulnerabilities. A concept model, a term introduced by Richardson [25], serves to illustrate a systems view of a problem through formal simulation. We use the tools of system dynamics [26] to identify how elements of the problem are causally linked to produce the problem behavior under study. Behaviors may be empirically observed or constructed from theory. Formal simulation requires the explicit specification of the components of the problem that generate the behavior, and in turn makes this specification concrete and open for critical examination.

Further, concept models help identify what data is important for investigation and raise awareness about potential counter-intuitive behavior.

5.1 Reference Mode

One important aspect of developing dynamic simulation models is the representation of system behaviors as they evolve over time. This is both an aspect of theory development and model refinement: Problem definition starts with the depiction of how critical variables behave. These depictions are drawn from the understanding of experts, hard data, or both, reflecting the robust and often contradictory perceptions of reality found in complex systems [26].

In this particular problem, we considered the abstract problem of vulnerabilities within a single software product. The unknown vulnerabilities embedded in this product are ultimately discovered by Black Hat and White Hat hackers, operating in legal (LM) and black markets (VBM). We assume that the fraction of vulnerabilities discovered will monotonically increase as the hackers pore over the software (Figure 1). We also assume that having both a legal and a black market will increase the speed at which vulnerabilities will be found. Arguably, paying hackers provides incentives for their efforts and draws new individuals into the search, in essence a multiplier effect based on the original incentive structure (the cross-hatched area).

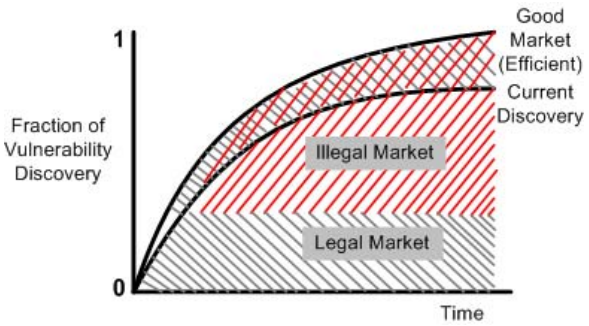


Figure 1 Hypothesized reference mode

5.2 Model Description

Our concept model's objective is a formal representation of the structure of a vulnerability marketplace that produces this postulated behavior.

The major constructs of SD models are stocks and flows. Stocks, represented by boxes, are accumulations of physical items or information over time. Flows, represented by double line arrows, represent the movement of these items among stocks, captured as a rate over time. In addition, information about the size of stocks or flows is available. In most cases we find that information about the state of stocks and flows feeds back into the system and changes the size of future flows. These information flows, depicted by single line arrows, form loops that reinforce or suppress future changes in the system [26].

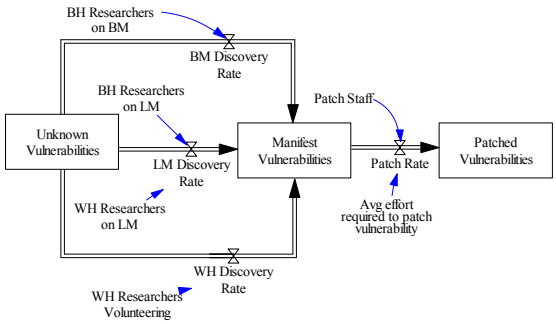


Figure 2 Vulnerability Finding and Trading

The structure of this *Vulnerability Finding and Trading* model includes three linked stocks representing the migration of vulnerabilities among three states (Fig. 2). When the software product is released it contains some number of unknown vulnerabilities. White Hat and Black Hat hackers attempt to uncover these vulnerabilities and make them manifest. White Hat hackers discover vulnerabilities and provide them to developers or to open non-profit vulnerability sites. Black Hat hackers sell their findings for our hypothesized black market. Later in the paper we will activate a third channel, representing a legal market for vulnerability exchange.

Once a vulnerability is manifest, it remains until software developers develop patches that address the vulnerability. Moving manifest vulnerabilities forward to a patched or hardened state is important, as software consumers are exposed for the time that any vulnerability is manifest and unpatched. In this model, the speed of patching depends on the number of patch staff and the effort required to install the patches. For the purposes of this concept model, we ignore the concerns about delays in the application of patches on the consumer side for fear of side effects.

The goal of a legal vulnerability market is to move Black Hat hackers (or researchers) out of the black market (BM) channel and into a legal market (LM) channel of some form, with either full or responsible disclosure of vulnerabilities to vendors. This movement is enabled by a combination of incentives that attract the attention of the Black Hats and pay them for their efforts. We have chosen to model this as a form of technology adoption [26], where after the launch of a legal market program, the prospect of legitimate payments and word of mouth dissemination of the success and safety of the new process lures some or all of the Black Hats over to the legal market (Figure 3). We continue to identify these actors as Black Hat, as they do have the option of returning to the illegal marketplace. Our observations of the VBMs support these assumptions. We found hackers that simultaneously deal with legal and black markets, share experiences and provide an evaluation of legal markets.

The rate of movement is governed largely by the price sensitivity of Black Hats to the offering of the market and their unknown strike price. Some of the individuals who enter the market may return; others may never try it. This approach allows us to simulate the behavior of a continuous marketplace without having to model individual transactions.

While this model represents an abstraction, it provides a starting point for examination of the effects of introducing a legal market. It is largely an "open loop" model, as it neglects much of the theorized complexity present in a true model of the vulnerability problem. The only feedback in place is the migration of black hat hackers and the effects of that migration of vulnerabilities. As we shall see, even this small structure provides some insight, including some counter-intuitive insight.

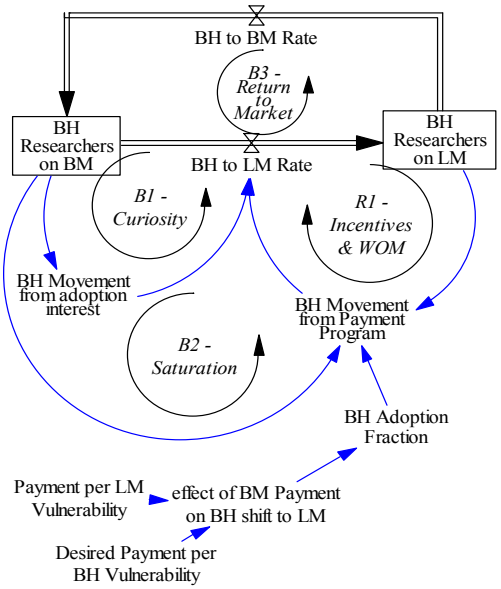


Figure 3 Adoption of Legal Markets By Black Hat Hackers

5.3 Simulation

For our initial runs of the simulation we examined several scenarios. The first scenario (Current), represents the absence of a legal market for overtly compensating hackers for their work. A second scenario (Legal Market) assumes activation of the legal market. We assume the same number of Black Hat and White Hat hackers, and that they have the same skills. As we are modeling their efforts against a single software product, we assume a fixed number of unknown vulnerabilities (1000) and a product lifetime of two years.

As expected, the cumulative of vulnerabilities discovered over time increases towards the maximum. In the absence of a legal market, with the same number of researchers and the same productivity, vulnerabilities are split evenly (Figure 4a). When a legal market is introduced, and price expectations are met, we see that there is the expected migration to the legal market (LM) (Figure 4b). As productivity does not change and no new researchers come into the market (a constraint built into our initial formulation), the slopes are identical.

The secondary effects of the successful movement of Black Hat researchers to a legal market are a bit more interesting. We assume that patching vulnerabilities discovered through the black market is more challenging than those discovered through legal or open market

channels. Black market vulnerabilities are manifested through attacks or extortion threats. The others are manifested through reports to vendors, or postings on web sites, presumably with more information about how the problem was identified. When a legal market is open, more information is available, as researchers may be expected to provide documentation, not just the exploit. This in turn means that it will be easier to patch vulnerabilities in when a legal market exists. This in turn reduces the time that vulnerabilities are manifest and unpatched, reducing consumer exposure.

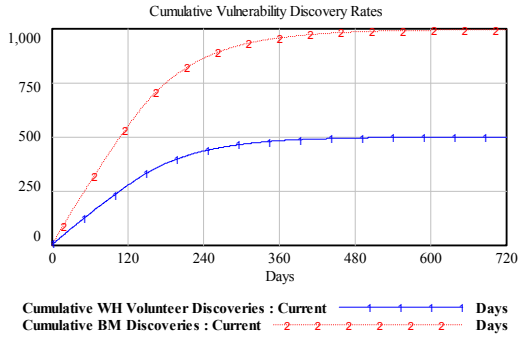


Figure 4a Vulnerability Discovery - No Legal Market

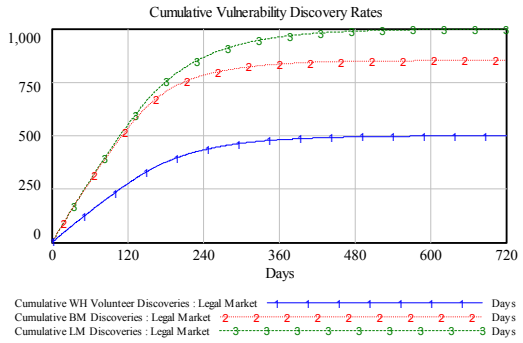


Figure 4b Vulnerability Discovery - Legal Market

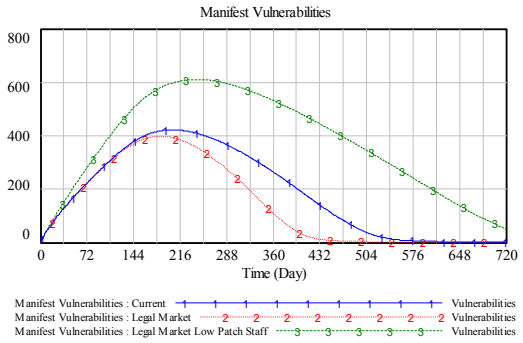
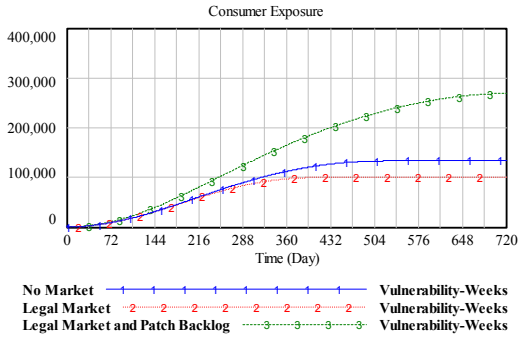


Figure 5a Manifest Vulnerability Discovery



The patch rate also depends on having sufficient resources to patch manifest vulnerabilities as they arise. If there are insufficient resources for this task, then the backlog of manifest vulnerabilities grows (Figure 5a, line 3), extending the period of risk and consumer exposure (Figure 5b, line 3).

There is therefore an unanticipated side effect worth considering. Creating a legal market for vulnerabilities may increase software hazards, even when controlling for the number of hackers and their productivity. Firms receiving information about vulnerabilities must act on them or risk increasing exposures. This is an exemplar of the "shifting the burden" archetype identified by Kim [27] and Senge [28], where changes in one part of a complex system have unanticipated downstream effects.

In the absence of sufficient resources dedicated to fixing security patches, manifest vulnerabilities accumulate. The more vulnerabilities, the greater risk to the vendor and customers is. While a vulnerability may not always be turned into an attack, long-standing problems might attract attention. In the case of bots, where a successful attack on one network might generate other attacks, the overall effect of neglected flaws may reach beyond the boundary of the organization and affect many others.

6. Conclusion

Do vulnerability black markets exist, or are they the creation of media and security companies? After collecting data from various websites and discussion forums for months, we believe that there is evidence that such markets exist and remain viable. Our initial examination of data indicates that these forums have a lifecycle and behaviors that support their need for both visibility and invisibility. Participants have to spend time establishing their reputation before their contributions are recognized. Moderators regularly clean and purge their systems of non-contributors, either by removing users or restarting the site. Much of the transaction detail is hidden in the privacy of personal messaging, but solicitations are open. It appears that there must be some reason that these sites perpetuate, so we treat them as real. In turn it becomes useful to examine conditions under which participants in these black markets can be turned to serve more conventional needs while not adding risks to the environment.

Our concept model captures an abstract example of parallel legal and illicit markets. While some authors have focused on developing the conditions needed for efficient and cleared markets, we look instead at the process by which transitions from black to white markets develop and the resultant effects on overall software quality. We find that under circumstances where vulnerability discovery is accelerated, it also becomes necessary to speed the development of patches for these flaws. If this is lacking, more manifest vulnerabilities remain, which in turn may increase the exposure of customers and vendors. Such counter-intuitive results argue for careful examination of the context and grounding for implementing legal markets as a counter for vulnerability black markets.

References

[1.] Hoglund, G. and G. McGraw, *Exploiting Software: How to Break Code*. 2004, Boston: Addison-Wesley.

[2.] IBM. *IBM Internet Security Systems X-Force 2006 Trend Statistics*. 2007 January [cited; Available from: http://www.iss.net/documents/whitepapers/X_Force_Exec_Brief.pdf.

[3.] PandaLabs. *Quarterly Report PandaLabs*. 2007 July 15, 2007 [cited 2007 12 September]; April-June 2007:[Available from: http://www.pandasecurity.com/.

[4.] Symantec, *Symantec Global Internet Threat Report: Trend for July - Dec 07*. 2008.

[5.] Finjan Inc. *Web Security Trends Report*. 2006 [cited 2006 September 20]; Available from: http://www.finjan.com/Content.aspx?id=827.

[6.] Clinard, M.B., *The Black Market: A Study of White Collar Crime*. 1969, Montclair, New Jersey: Patterson Smith.

[7.] Radianti, J. and J.J. Gonzalez. *a Preliminary Model of The Vulnerability Black Market*. In *the 25th International System Dynamics Conference* 2007. Boston, USA.

[8.] Ozment, A. *Bugs Auctions: Vulnerability Market Reconsidered*. In *Workshop of Economics and Information Security (WEIS)*. 2004. Mineapolis, MN.

[9.] Böhme, R. *A Comparison of Market Approaches to Software Vulnerability Disclosure*. In *International Conference, ETRICS 2006, LNCS 3995* 2006. Freiburg, Germany: Springer-Verlag Berlin Heidelberg.

[10.] Miller, C. *The Legitimate Vulnerability Market: the Secretive World of 0-day Exploit Sales*. In *Workshop on Economics of Information Security*. 2007. Pittsburgh, USA.

[11.] Sutton, M. and F. Nagle. *Emerging Economic Models for Vulnerability Research*. In *The Fifth Workshop on the Economics of Information Security (WEIS)*. 2006. Robinson College, University of Cambridge, England.

[12.] Naraine, R. *Researcher: WMF Exploit Sold Underground for $4,000* 2006 [cited 2007 September 15]; Available from: http://www.eweek.com/article2/0,1895,1918198,00.asp.

[13.] Naraine, R. *Hackers Selling Vista Zero-Day Exploit*. 2006 [cited 2007 June 2]; Available from: http://www.eweek.com/print_article2/0,1217,a=196573,00.asp.

[14.] Naraine, R. *Price War: iDefense Doubles Bounty for Security Flaws* 2005 [cited 2007 April 28]; Available from: http://www.eweek.com/article2/0,1895,1841268,00.asp.

[15.] Schechter, S. *How to Buy Better Testing: Using Competition to Get The Most Security and Robustness for Your Dollar*. In *Infrastructures Security Conference*. 2002. Bristol, UK.

[16.] Kaplan, D. *Threats for $ale*. SC Magazine 2006 [cited 2006 August 4]; Available from: www.scmagazine.com/us/news/article/556843/threats-ale/.

[17.] Franklin, J., et al. *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants*. In *14 th ACM Conference on Computer and Communications Security (CCS)*. 2007. Alexandria, VA, USA.

[18.] Zhuge, J., et al. *Studying Malicious Websites and the Underground Economy on the Chinese Website*. Honeyblog 2007 [cited 2008 February 25]; Available from: http://honeyblog.org/archives/2007/12/summary.html.

[19.] Akerlof, G.A., *The Market for "Lemons": Quality Uncertainty and Market Mechanism*. The Quarterly Journal of Economics, 1970. **84**(3): p. 488-500.

[20.] Radianti, J., E. Rich, and J.J. Gonzalez. *Using Mixed Data Collection to Uncover Vulnerability Black Markets*. In *Workshop of Information Security and Privacy*. 2007. Quebec, Canada.

[21.] Luna-Reyes, L.F. and D.L. Andersen, *Collecting and analyzing qualitative data for system dynamics: methods and models*. System Dynamics Review, 2003. **19**(4): p. 271-296.

[22.] Gross, G. *Internet Currency Firm Pleads Guilty to Money Laundering*. PCWorld 2008 [cited 2008 July 23]; Available from: http://www.pcworld.com/businesscenter/article/148720/internet_currency_firm_pleads_guilty_to_money_laundering.html.

[23.] Higgins, K.J. *Bucks for Bugs*. 2006 [cited 2007 July 20]; Available from: http://www.darkreading.com/document.asp?doc_id=99518.

[24.] Landesman, M. *Malware Revolution: A Change in Target*. 2007 [cited 2007 April 10]; Available from: http://www.microsoft.com/technet/community/columns/secmgmt/sm0307.mspx.

[25.] Richardson, G.P. and D.F. Andersen, *Teamwork in Group Model Building*. System Dynamics Review, 1995. **11**(2): p. 113-137.

[26.] Sterman, J.D., *Business Dynamics: Systems Thinking and Modeling for a Complex World*. 2000, Boston: Irwin/McGraw-Hill.

[27.] Kim, D.H., *Introduction to Systems Thinking*, in *Innovations in Management Series*. 1999, Pegasus Communications: Waltham, MA.

[28.] Senge, P.M., *The fifth discipline : the art and practice of the learning organization*. 1st ed. 1990, New York: Doubleday/Currency.