A Quest for a Framework to Improve Software Security: Vulnerability Black Markets Scenario

Jaziar Radianti
(jaziar.radianti@uia.no)

Jose J. Gonzalez
(jose.j.gonzalez@uia.no)
Security and Quality in Organizations
University of Agder, Service Box 509
4898 Grimstad, Norway

Eliot Rich
(e.rich@albany.edu)
School of Business, University at Albany
State University of New York
1400 Washington Avenue
Albany, NY 12222

Abstract

The discovery and management of software vulnerabilities after a product is released to the public is an important element of improving software quality and stability. The discovery of vulnerabilities enables exploitation and stimulates the development of patches or other protections, which in turn may or may not be deployed by product users. Various approaches have been developed to facilitate discovery and reduce vulnerabilities, including mechanisms for secret reporting, full-disclosure, responsible disclosure, and market-driven approaches. Our research focuses on the development of vulnerability black market which emerged as Internet-enabled communication among malicious hackers as a means to sell exploits and malware that take advantage of software flaws. The model in this paper draws on empirical observation on black markets and theories of market-based activity to generate a dynamic simulation model of vulnerability black market structure and behavior over time The model results suggest that efficient legal markets may attract malicious hackers to enter the legal markets and may reduce their likelihood to be involved in vulnerability black markets. We also find that adopting better patching management on the vendor side may mitigate the abuse of software vulnerabilities.

Key Words: *Information Security, Software Vulnerability, System Dynamics, Vulnerability Black Market,*

1. Introduction

The availability of software vulnerabilities through black market channels appears to be growing in importance over time. Previous studies on vulnerability black markets include Internet black market commodities (Penenberg 2008; Symantec 2008a, 2008b; Franklin et al. 2007), estimation of malicious actor's earnings (Franklin et al. 2007), and the structure of a malicious website in China (Zhuge et al. 2007). Most of them investigate the operation of the underground economy. These studies, along with the works cited below provide circumstantial evidence that such markets are tenable. The existence of such markets, for nuisance vulnerabilities or serious disruptions, creates a technology hazard of unknown proportions.

The continued existence of these markets and mitigation of their effects are rooted in the approaches employed for discovering and correcting software vulnerabilities by those affected by the state of software security. Vulnerabilities in post-release move through three stages: In the simplest and most benign case, a discovery of a vulnerability is followed by its announcement to the public along with a patch provided by the vendor or by a third party, such as an anti-virus vendor. Software vulnerabilities have such a high economic or disruptive value that skilled hackers attempt to exploit them in any of their different statuses—discovered, announced and patched. The decisions and activities of vendors, third party security companies, black hat and white hat hackers and the public create delays and unintended outcomes and create opportunities for black markets to remain active.

One proposed management scheme supporting continuous licit vulnerability discovery, rewards the discoverer when they report their findings to either vendors or third parties. Supporters of this approach believe that it can be efficient and self-regulating, drawing hackers from the 'black' to the 'white' sides of the problem (Zorz 2003). Critics argue that such a market would increase demands for compensation and increase the number of unpatched vulnerabilities in the wild. In addition, as such discoveries are easily transferred and replicated, there may be no market mechanisms preventing resale of vulnerabilities to both the white and black market before a patch is ready (Ozment 2004). Thus the question of market dynamics remains open: Will the proposed market structure create an environment that exerts better control over software vulnerabilities and improve quality, will it have no effect save enriching hackers, or will it serve to further exacerbate the problem?

In this paper we develop a dynamic model that captures the structure of vulnerability discovery through white and black markets. The model allows us to examine if the market approach leads to more efficient vulnerability discovery and encourage more discoveries; to simulate and test the policies best suited to vulnerability black market problems, and to recommend further remedial strategies to prevent vulnerability black market proliferations; and to communicate counterintuitive dynamic outcomes of the vulnerability black market proposal.

2. Literature

In a previous work we have defined a vulnerability black market as "an arena or any arrangement for illegal selling and buying activities to trade vulnerability exploits and malware or any products taking malicious advantage of the weaknesses in software and computer networks" (Radianti and Gonzalez 2009). Software vulnerabilities are "bugs and flaws (caused by programming errors) that give rise to exploit techniques or particular attack patterns."[1] Software vulnerabilities might originate from a newly introduced software flaw, exist from the first day of release of the products, or unintentionally derive from a fix for a security issue in a previous version (NIST 2006).

[1] See further: Landwehr et al. (1994), Du and Mathur (1998), Seacord & Householder (2005) and Engle (2006) et al. (2006).

Prior works on a policy to manage vulnerability discoveries covered a wide spectrum of operating maxims, including proposals to keeping the existence of the vulnerability hidden to fully disclosing it to the public (Schneier 2007). Others propose that vulnerability announcements be delayed for a period after discovery to permit the development of patches or remedies (Organization for Internet Safety 2004; Cavusoglu, Cavusoglu, and Raghunathan 2005). This proposal, called "responsible disclosure," was found empirically to be less efficient than instantaneous disclosure, as faster disclosure forces vendors to provide quick patches (Arora et al. 2004) and appears to decrease the vendor's stock market price (Telang and Wattal 2007). An institutional solution for managing the identification and disclosure of vulnerability along the lines of a Computer Emergency Response Team (CERT) has also been proposed. Such an organization would permit researchers to report the details of their discoveries to trusted parties who would actively coordinate a solution (Schneier 2000; Arora, Telang, and Xu 2008).

Researchers with the expertise required to discover software vulnerabilities are a significant and fast growing group. Lack of reward for security researchers who found vulnerabilities generated the idea of a market-based discovery approach (Zorz 2003), such as a compensated discovery and "not-for-free-disclosure policy".

Theoretical models for economically-efficient vulnerability markets include different contexts such as competition among testers (Schechter 2002), auction (Ozment 2004) and cyber insurance (Böhme 2006). Vulnerability market models are addressed by Sutton and Nagel (2006) based on recent practices. Kanan and Telang (2005) theorized that a regulated market performs better than an unregulated market-based mechanism for channeling vulnerabilities, compared to a passive CERT-type mechanism. However, they recommend a combined between CERT-type and market-based approach, i.e. to let CERTs fund vulnerability discoveries because it provides better social welfare.

Skepticism about the effectiveness of efforts towards continuous vulnerability discovery leads Rescorla (2005) to propose user education, patching improvement and response technology as keys for improving security. Attackers are familiar that many end users are reluctant to update their machines immediately. Various successful attacks on computer network actually abuse human vulnerability and employ social engineering technique.

Vulnerability black markets, where flaws and exploits are sold illicitly, have been identified by several recent authors (Miller 2007; Sutton and Nagle 2006; Ozment 2005, 2004). Empirical investigation found black markets as a place to buy and sell malicious tools, malware and exploits (PandaLabs 2007; IBM 2007, 2009, 2008). These markets may also sell other malicious tools and stolen data, such as botnets, spamming tools, obfuscators, CCs and CVV2s. Franklin et al. (2007) propose to disrupt such markets through active attacks on these sites, while others recommend the use of a broader legal approach, e.g. shutting down the malicious sites (Moore and Clayton 2008) and institutional cooperation to fight cybercrime (Rush et al. 2009)

As a part to understand the dynamic of the black market for vulnerabilities, economic theory offers a perspective on the black market in general. Prices and profits are central concepts in a free market operation that affect individual buyers and sellers' decisions (Perloff 2007). A few economic theories on black market exist (Boulding 1947; Bronfenbrenner 1947). Both authors assume that a black market is a result of an unsatisfied demand. Boulding derives his theory on black market supply and demand from an examination of wartime price regulation below the free market normal price. At a regulated price, demand will be higher than supply, thus leading to shortages. A black market emerges if buyers and sellers are willing to trade above the legal regulated price. The black market supply curve drawn from the legal regulated price is always steeper than the free market supply curve because of the higher risk of operating in a black market. Thus, the supply price

is always higher for each product in demand. Boulding (1947) introduces the possibility of penalties for participation in these markets. If law enforcement is more severe, the black market supply curve will be steeper (product price increases) and finally perfectly inelastic (black market price could exceed the free market price). Bronfenbrenner (1947) examines black market supply and demand behaviour in an imperfect market and assumes that the maximum demand in the black market is the excess demand over supply in the official market and no discrimination between rich and poor people in the rationing system. He suggests that the black market demand will be a ratio between excess demand and total demand at the regulated market (Bronfenbrenner 1947).

A few other black market theories and critiques emerge after Boulding and Bronfenbrenner, e.g., from Michaely (1954), Nordin and Moore (1947) and Gönensay (1966). Michaely (1954), e.g. points out inconsistency between the assumption and the implication of the black market supply demand curve construction. The assumption implies that supplier will shift from regulated market to black market when the black market price rises. However, the demand curve construction implies an unchanged excess demand at the regulated price.

Apparently, the aforementioned black market theories may not be satisfactory for our case. Software vulnerability black markets differ from the supply, demand and price behavior found for other goods. The stigma attached to vulnerability black markets is not because they operate outside the regulated price, but because commodities traded on them are often used for attacking computer networks. The price of some vulnerability black market goods, e.g. exploits or malware, can lose their value immediately when they become public or vulnerabilities they target are patched. Although available, few will purchase them. In addition, the more secret the malicious tools, the higher their value. Thus, price alone might be inadequate to explain such market behavior.

A methodology that is able to capture various features (time delays, non-price operation, non-linearity relationships) in such black market is required. The System Dynamics approach offers this capability (Sterman 2000; Richardson and Pugh 1981). The method has been used for many years to explain macro and microeconomic behavior. Meadows (1970) combined economic theory and system dynamics to explain the dynamic of commodity cycle model and to incorporate price elasticity into his model. Mass (1980) used stock and flow variables to explain economic supply and demand. Sterman (2000) demonstrates how price serves as a negative feedback loop to govern supply and demand.

However, Sterman also argues that not all markets are regulated through price alone, particularly in an institutional setting (ibid, p.170). In this black market case, price and profit play a role but do not dictate the quantity of supply or demand. The marketplace works similarly to the marketplace where the operations depend upon the availability of goods to offer instead of the interaction between demand and supply that determines the market price and the quantity of a good or service that is bought and sold. Hence, it operates as supply and demand in most institutions or particular type of organization that have no price-mediated markets. Availability, politics, perceived fairness and other administrative procedures serve are examples of non-price factors to mediate resource allocation. Availability is an important competitive variable in many products markets, and firms regulate production in response to inventory adequacy and delivery delay (Forrester 1961; Sterman 2000). This study uses the “availability” concept to model and simplify supply and demand in vulnerability black markets.

3. Problem Definition

Despite improvements to software development in various stages during testing in the pre-release phase as well as in the post-release phase, vulnerabilities are continuously being discovered. The cost of damage to computer security incidents exploiting the software weaknesses is growing over time. Is it possible to improve the software quality? Inadequate

software testing (Tassey 2002), more skilled hackers, advanced exploiting techniques (Solomon and Chapple 2005; Hoglund and McGraw 2004) and the availability of online underground forums and black markets are responsible for the increasing computer incidents (Symantec 2008a). This creates a policy design problem, as the more attractive solutions may improve the software quality in the short run but ultimately unintended consequences appear and prevent security improvements from being met (Anderson 2001).

3.1. Time Unit and Time Horizon

To choose a *time unit*, a few aspects should be considered so that the model can capture enough dynamics of the problem to be addressed in this study. For example, a number of variables may be sensitive to the number of days rather than weeks, months or years, if we are interested in seeing how fast an exploit is created (some take one day or less), which explains the rapid expansion in the window of vulnerabilities. However, since our focus on software vulnerabilities is from their discovery until they are patched, a monthly time unit is sufficient to observe the behavior of the most important variables.

Regarding the *time horizon*, 168 months (or 14 years) is adequate to capture the dynamics of most software vulnerability problems and vulnerability market behavior. The average life cycle of software is around three years, from launch until out-of-date. However, to observe the dynamics of the consequences of policy intervention, impacts on the black markets and vulnerability black markets, and improvements in software security, we need a longer timeframe. In addition, the first 84 months of our model are historical record. Thus, the selected timeframe of 168 months is adequate to capture the longest time delays in the system. For example, according to Arora et al.'s measurement (2006) the average age of exploited vulnerabilities is 899 days or around 30 months.

3.2. Reference Mode

Defining a vulnerability problem by graphing it over time allows us to see the dynamics of it. Reference modes are created to help the modeler to conceptualize the model, facilitate the selection of its basic causal structure and validate it (Richardson and Pugh 1981; Randers 1980). We start by referring to the life cycle of vulnerabilities—a process of birth, discovery, disclosure, fixing and obsolescence of vulnerabilities. Some researchers model the life-cycle of a vulnerability as a bell-shaped curve as a result of growth, when vulnerability is announced and decay when vulnerability is patched (Arbaugh, Fithen, and McHugh 2000; Browne et al. 2000; Howard 1997; Lipson 2002; Rescorla 2005).

Schneier (2000) plots a vulnerability's life cycle against the risks, based on different states of the vulnerability over time, while Arbaugh et al. (2000) plots it against the intrusion rate. Lipson uses it to reveal the intensity of exploit spread. Rescola (2005) models the life cycle on the numbers of vulnerable machines. He distinguishes black hat and white hat discovery process, and assumes that disclosure and fix occur simultaneously. The difference between the former and the latter is that in a black hat discovery model, the private exploitation has already started before public exploitation, i.e. between discovery and disclosure time.

The similarity among their curves is that they reveal no risks, vulnerable machines, intrusions, exploits when no one discovers the vulnerabilities. The risks, vulnerable machines, intrusions or exploits gradually increase when people find the flaws. Sudden jumps in the life cycle curve occur as the vulnerabilities are announced and then decrease when they are patched. Wiik et al. (2004) have built a system dynamics model that follows this vulnerability life cycle reference mode.

Statistics from CERT, OSVDB and CVE[2] confirm that the average number of reported vulnerabilities increase over time. OSVDB recorded 2,357 reported vulnerabilities in 2002, and then an almost fourfold increase by 2006 to 10,709, before decreasing slightly in 2007 and 2008. Although the data from CERT and CVE show a slight difference in the number of vulnerabilities, but these two public vulnerability databases demonstrate a similar trend, i.e. peaking in 2006 and decreasing slightly in 2007 and 2008 (See Table 1). Between 2002 and 2007 CERT and CVE recorded 27,315 and 34,456 vulnerabilities respectively. From 2002-2008, total vulnerabilities documented by OSVDB were 45,045.

Table 1
Reported Vulnerabilities 2002-2008

Year	Vulnerabilities		
	OSVDB	CERT	CVE
2002	2,372	4,129	1,527
2003	2,489	3,784	2,156
2004	4,816	3,780	2,451
2005	7,549	5,990	4,933
2006	10,709	8,064	6,608
2007	8,922	7,235	6,515
2008	8,188	6,058	5,634

Information on vulnerabilities channelled through legal markets was collected from VCP (Vulnerability Contributor Program) and ZDI (Zero Day Initiatives)[3]. Monthly auctions in WSL (WabiSabiLabi) which began operating in July 2007 were also monitored. Until October 2008, WSL's market history recorded thirty-four vulnerabilities, with thirty-two of them traded in 2007 and the two remaining in 2008[4]. However, WSL is reported to have shut down in November 2008 (Higgins 2008; Lemon 2008), and the website has been temporarily unavailable. No public information was available about the number of vulnerabilities obtained by DACP (Digital Armaments Contributor Program), Core Security and iSight Partners [5]. In addition, it is not known whether the buyers particularly in WSL and DACP reported to the affected vendors or not. Platinum subscription in DACP and full-right on vulnerabilities obtained from WSL give the buyers an exclusive right on the bought vulnerabilities. Hence, only legal market data from VCP and ZDI was available. The annual data from legal markets (LMs) and the annual data from OSVDB[6] (2002-2008) are given in Table 2.

On average, the legal markets (LMs) vulnerabilities account for 1-3% of all vulnerabilities discovered from 2002-2008. Although the number of reported vulnerabilities decreased slightly in 2007 and 2008, the proportion of legal markets to overall discoveries increased. Legal markets could be attracting more attention from security researchers.

[2] CERT (Computer Emergency Response Team, *see* www.cert.org) catalogues data from two sources—public report and direct report. OSVDB (Open Source Vulnerability Database, *see* www.osvdb.org) obtains data from various sources, e.g. CVE, Bugtraq, Nessus, Snort Filter, Secunia, Microsoft Bulletin and CERT. CVE (Common Vulnerability Exposure, *see* http://nvd.nist.gov) also collects information from other public forums such as CERT, ISS (Internet Security Systems), Bugtraq.

[3] *See* http://labs.idefense.com/vcp and www.zerodayinitiative.com

[4] www.wslabi.com, retrieved 15 July 2008

[5] *See* www.digitalarmaments.com, www.coresecurity.com, https://gvp.isightpartners.com.

[6] The information from legal markets will also be aggregated in the database has been confirmed by OSVDB through email communication, May 2009. We also checked the CVE ID of vulnerabilities from VCP or ZDI randomly, to ascertain the legal market contributions are in OSVDB database.

Table 2
LM and Non-LM Vulnerability Discovery

	Total Vulnerabilities (a)	LMs (b)	Non LM Sources (a-b)	LM/Total (%)	Non LM/Total (%)
2002	2 ,372	40	2,332	2	98
2003	2 ,489	35	2,454	1	99
2004	4 ,816	81	4,735	2	98
2005	7 ,549	151	7,398	2	98
2006	10 ,709	141	10,568	1	99
2007	8 ,922	307	8,615	3	97
2008	8 ,188	261	7,927	3	97

In line with the monthly selected time unit, the reporting rate and the number of cumulative vulnerabilities are summarized in Figures 1a and 1b, from 2002 to 2008. In Figure 1a, the trend of the monthly reported vulnerabilities gradually increased from 2002 and peaked around 2006. Afterwards, it decreased slightly from May 2006 onward. A few questions arise, since this decreasing trend does not necessarily indicate fewer discoveries, or that newer software is becoming more secure. Does it occur because of underreporting (reluctance from security researchers to report, delays in verification and publication) or does the market-based reporting alternative account for it?

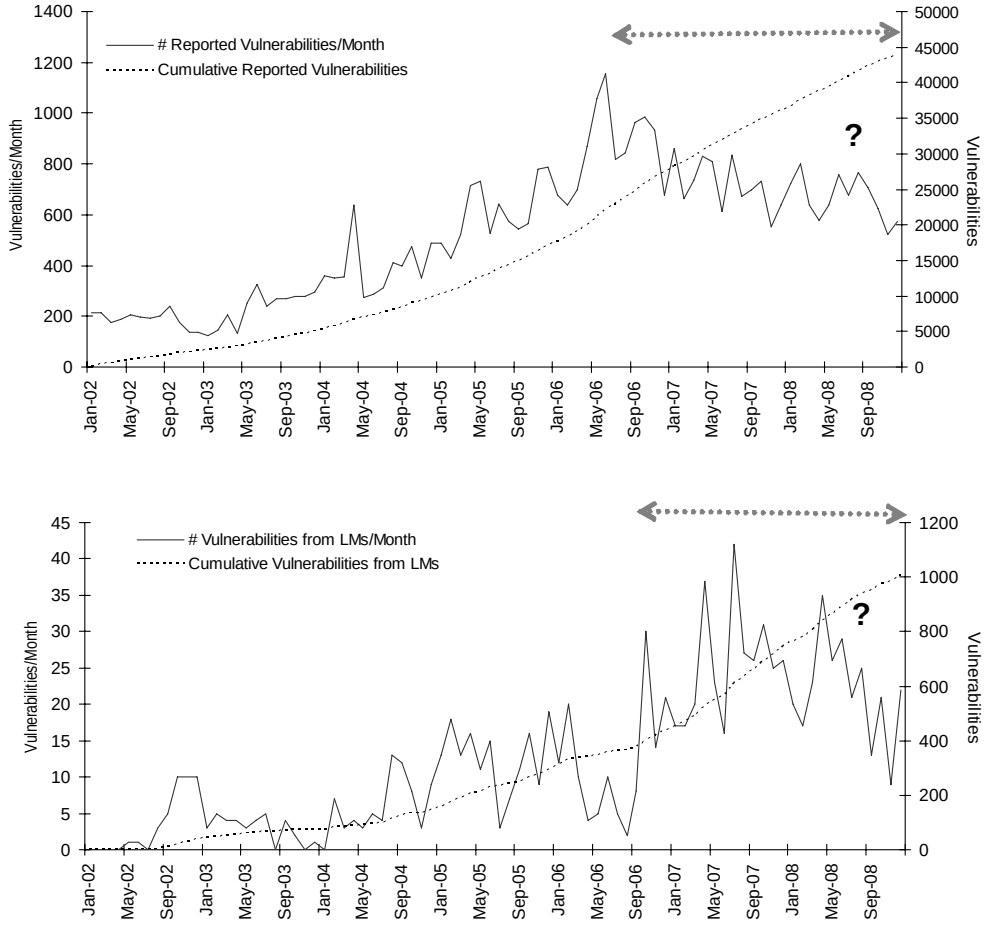

Figure 1a (Above) Non-Legal Market Reported Vulnerabilities and Figure 1b (Below) Vulnerabilities Obtained from Legal Markets

On the other hand, the trend of the monthly market-based vulnerabilities (Figure 1b) increased from 2002 and peaked in 2007. However, a decrease occurred from mid 2007 onward. No significant development happened during this period. More questions arise. Will market-based discoveries continue stable, increase, or decrease over time? Is there a tipping point where the trust of the security researchers on the market-based practices begins to erode, and hence hinders market development? The previous example of WSL rumored to be shut down indicates that not all types of legal markets can easily gain the trust of security researchers. Part of the discussion of the WSL failure made mention that such unknown vulnerabilities marketing model posed a risk of vulnerability rediscoveries thus depleted their original value (Higgins 2008).

In brief, there are three possible scenarios of for future vulnerability discoveries: increase (desired), steady (undesired) or decrease (feared). A diminishing trend would not be feared if it occurred concurrently with a decreasing trend in computer incidents. Unfortunately, statistics reveal the opposite for computer security incidents (Richardson 2008; IBM 2009).

Table 3 shows that in the period from 2002 to 2008, the highest number of discovered vulnerabilities (1,158), occurred in 2006. The average reported vulnerabilities for this year though were only 860 per month. Moreover, the average monthly reported vulnerabilities for 2002-2008 were 524. The average number of vulnerabilities has tripled from 190 in 2002 to 667 in 2008.

Table 3
Information on Reported Vulnerabilities

Period	Monthly Average # vulnerabilities	Min # Monthly Reported vulnerabilities	Max # Monthly Reported vulnerabilities
Jan – Dec 2002	190	137	241
Jan – Dec 2006 (extreme year)	860	637	1,158
Jan – Dec 2008	667	521	800

Table 4
Information on Vulnerability Exploits and Patches (2002-2008)*

	2002	2003	2004	2005	2006	2007	2008
# Exploit Available (a)	542	752	1,849	2,215	3,433	2,606	3,631
# Exploit Rumored/Private (b)	57	72	132	674	671	160	38
Total Vulnerabilities With Exploit (a + b)	599	824	1,981	2,889	4,104	2,766	3,669
Total Reported Vulnerabilities (TRVs)	2 ,372	2 ,489	4,816	7,549	10,709	8,922	8,188
Exploit Available/TRVs in a given year (in %)	23	30	38	30	32	30	40
Exploit Rumored/TRVs in a given year (in %)	2	3	3	8	6	1	0
Total Exploit/TRVs in a given year (in %)	25	33	41	38	38	31	40
Patched Vulnerabilities	22	35	24	36	144	484	2,367
Patched/TRVs in a given year (in %)	0.1	2	4	5	1	5	29

**) Source: OSVDB*

Likewise, available historical records on exploited vulnerabilities show that the number of total exploited vulnerabilities rose from 25 to 40 percent over the last seven years (Table 4). In addition, IBM (2008) claims that independent researchers are almost twice as likely than research organization to have an exploit code published the same day as the vulnerability is disclosed.

An assessment of the number of exploited vulnerabilities is based on available statistical data, which may also include biases (e.g. incomplete vulnerability reports; the unreported available exploits, etc.) OSVDB provides the exploit's availability-based

vulnerabilities documentation. This recorded data can be used as a starting point for obtaining a more detailed picture of the addressed problem.

The difficult realm of analyzing vulnerabilities without any statistical data involves black markets, their development and the amount of relevant trading occurring on them. Figure 2a shows membership growth in vulnerability black markets, and Figure 2b the growth of black markets involved in vulnerabilities trading. Data was collected from observations carried out on twelve online black market forums from April 2006 to May 2008 (Radianti and Gonzalez 2009; Radianti, Rich, and Gonzalez 2009).

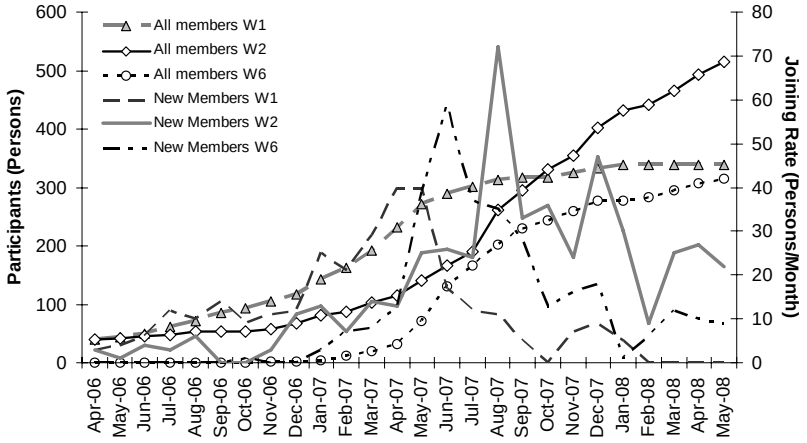

Figure 2a. Membership

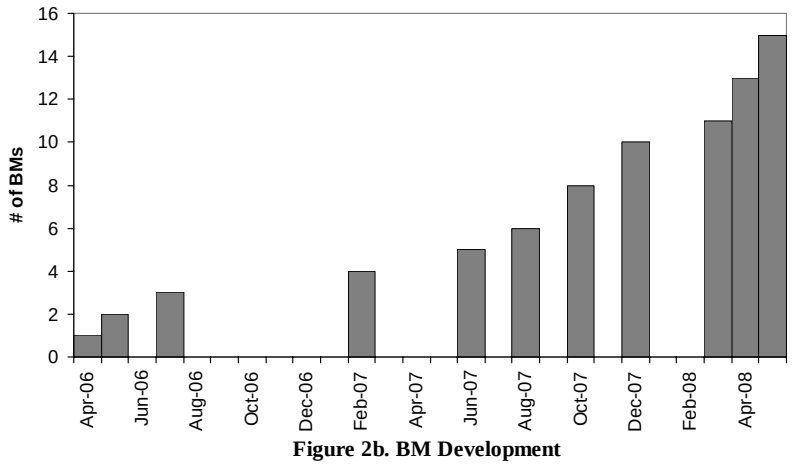

Figure 2b. BM Development

Figure 2

Vulnerability black markets develop in two ways—internally (Figure 2a) because of participant growth, and externally (Figure 2b) because more websites with a black market feature emerge (Radianti and Gonzalez 2009). Their size and access were unstable over the observed period for multiple reasons, including frequent intermittent website downtime. However, the observation results show that the number of members who joined the black market forums increased in the beginning before eventually declining. Cumulative membership developed in a limited way, following an S-shaped pattern (Figure 2a, right Y axis). Various exploits and malware were advertised on the forums observed, indicating that vulnerability appear to be increasing (Figure 2b).

The following graphs (Figure 3 and Figure 4) represent the hypotheses and inferences about the long term consequences of the software vulnerability discovery problem. Figure 3a shows the positive relationship between cumulative reported unpatched vulnerabilities and the number of zero-day and known exploits. The more vulnerabilities are discovered and published, the more exploits are developed and created. Further, the more vulnerabilities

needing to be patched, the smaller the percentage of the vulnerabilities being patched. Figure 3b shows the reference mode of the behavior effect of cumulative reported vulnerabilities over time. An increase in published vulnerabilities extends the influence of both vulnerability black markets and exploits. Thus, the greater the chance that a part of the exploits and malware will be traded on vulnerability black markets.

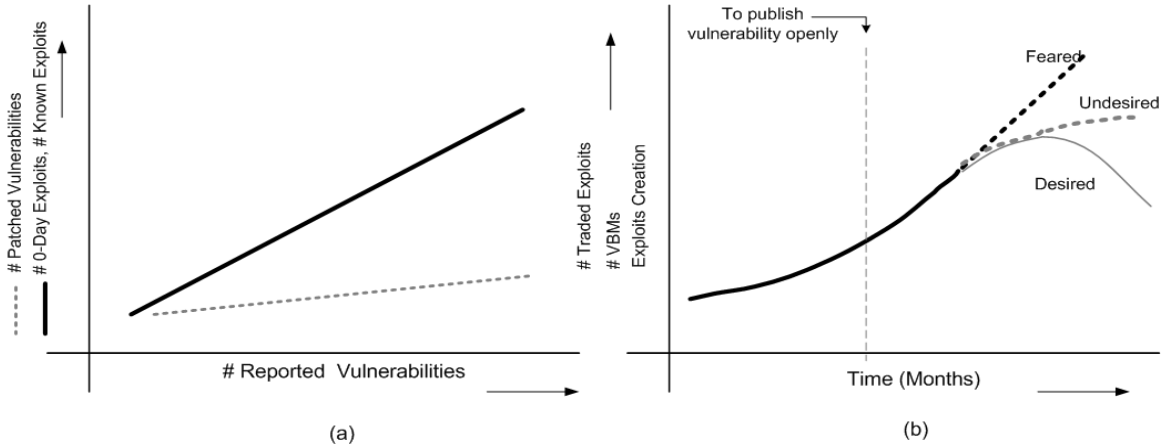

Figure 3

Figure 3a Figure 3b

Figure 4 illustrates the total percent of market reporting in the efficient market scenario. We assume that the total number of reported vulnerabilities in percentage from both legal market and non-market reporting in any given month is 100 percent. Efficient markets will contribute to vulnerability reporting, although perhaps, there is a trade-off where the number of *voluntary reported* might decrease slightly and the *market reporting* increases, compared to all reported vulnerabilities (Figure 4a).

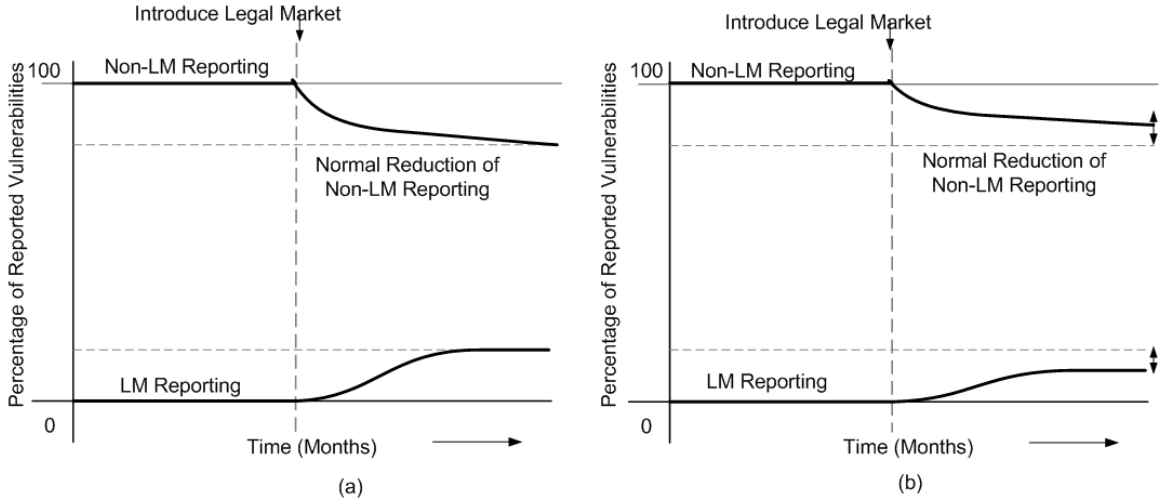

Figure 4

Figure 4a
The Percentage of Reported Vulnerabilities from LM and Non-LMs with Efficient Markets

Figure 4b
The Percentage of Reported Vulnerabilities from LM and Non-LMs with Inefficient Markets

On the other hand, inefficient markets can create an undesired or even feared outcome. In this scenario, the market does not trigger a significant change in the percentage of total reported vulnerabilities, and the voluntary reporting also goes down. In this undesired scenario, the reduction occurs because researchers are less motivated to find vulnerabilities

without compensation. The feared outcome happens if the decreasing trend in the percentage of both legal markets (LM) and voluntary (Non-LM) reporting is rooted in increasing vulnerability black market trading (Figure 4b).

3.3. The Modeling Purpose and the Dynamic Hypotheses

The modeling purposes are to understand the dynamics of the vulnerability black market development, to scrutinize whether efficient market mechanism contributes to greater vulnerability discoveries, and to examine factors underlying the successful and the failure of vulnerability markets and prevent further development of vulnerability black markets.

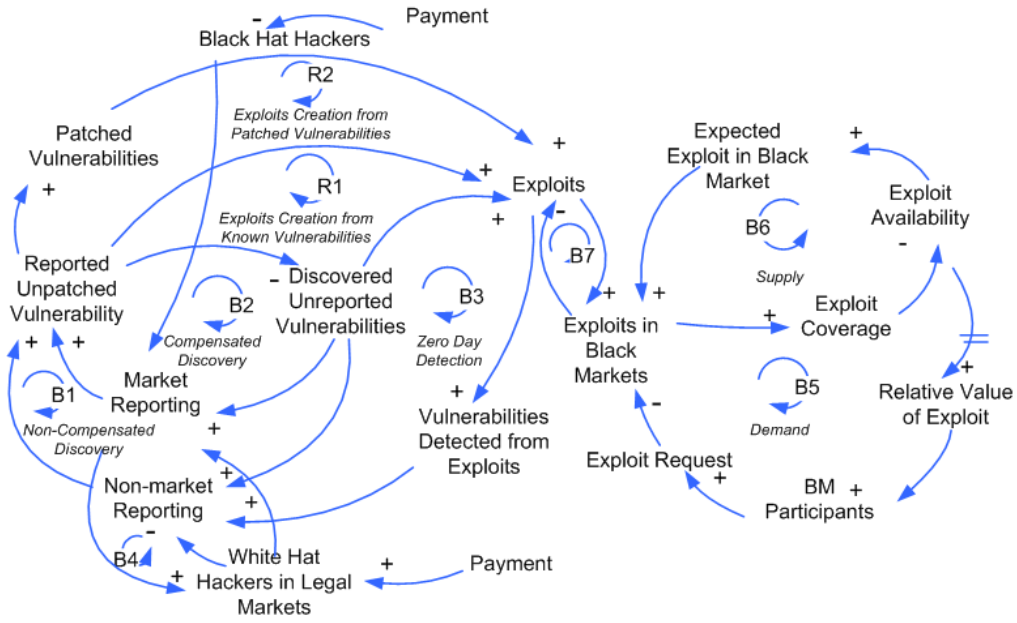

Figure 5
Dynamic Hypothesis

The focus here is on the dynamics of *reported unpatched vulnerabilities*, *market reporting*, *exploits* and *exploits supply and demand in BMs*. Information about vulnerabilities (because they are discovered or published) enables both exploits trading in black markets and vulnerability trading in legal markets. Increasing market-based discovery activities may erode the traditional fashion to report vulnerability without compensation. Thus, there is a trade-off between increasing market-based discovery and the decreasing trend of the voluntary reporting. Exceeding market-based activities force an involuntary downward pressure on overall vulnerability discovery activities, for example through bigger verification workload in legal market or longer time to detect exploits being used to attack computers.

We assume that the *reported unpatched vulnerabilities* are the most critical state where most risks arise, particularly the opportunity to create exploits or malware and trade them on black markets. In the *supply side*, exploits in vulnerability black markets indicate the exploit availability, determine the expected exploit trading, and furthermore increase the exploit creation. In the *demand side*, exploit availability spreads the attractiveness to the BM Participants. Once this attractiveness creates a demand, pushes trading, the exploit availability will decrease. These *supply* and *demand* loops represent the BM market mechanism. *Payment* in Figure 5 is assumed to be a main reason that generates the dynamics of aforementioned model.

4. Model Conceptualization

4.1. System Boundary

This model is an evolutionary result of previous work, where vulnerability black markets were looked at as conceptual models (Radianti and Gonzalez 2007b, 2007a, 2009; Radianti, Rich, and Gonzalez 2007, 2009). Archival Study, observation on black market forums and interview with a few security researchers were implemented in this study. Many factors affect the vulnerabilities problem addressed in this study and the most relevant factors are considered. For example, poor software quality and incentive failure frequently has been pointed out as among of causes of software vulnerability problems (Anderson 2001; Minasi 2000). It is excluded from our consideration since our focus is to look at the processes that happen between vulnerability discovery and patching. The boundary of the model is drawn in the Figure 6. Some factors are considered to be endogenous—those contained within feedback loops (thick solid-lines). One factor is exogenous—affects the state of the model system, but is not affected by other factors (a thin dashed-line). A few elements are omitted—those are completely absent from the model (dashed-lines).

There are five main sectors in Figure 6. *Chain of Vulnerability* and *Exploits Sectors* affect each other, because the lifetime of exploits to some extent depends on the secrecy of the vulnerabilities. Otherwise, vulnerabilities repeatedly are detected from the circulated exploits. Exploit creations sometimes spark exploit trading in black markets. *Security Researchers Sector* (describing people who are able to find vulnerabilities or create exploits, viruses and other malware) consists of the following groups of people: Black Hat Hackers (BHs) in Black Markets (BMs), White Hat Researcher Volunteers (WH) and Black Hat and White Hat Researchers in Legal Markets. Both legal markets and black markets often attract security researchers by providing monetary incentives. This last is captured in *Payment Sector*. The next subsection, a detailed description of the model will be organized in line with the sub sectors diagram.

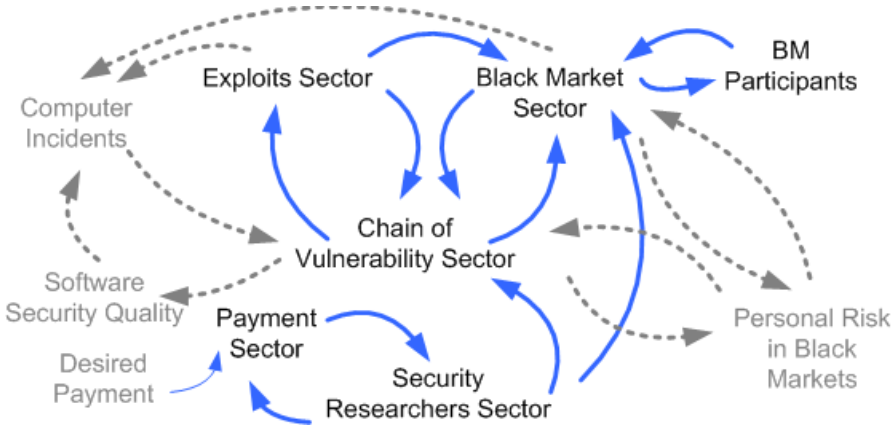

Figure 6
Main Sectors in a VBM Model

4.2. Feedback Structure

4.2.1. Vulnerability Chain Sector

The vulnerability chain sector contains four stocks: *Discovered Unreported Vulnerabilities*, *Vulnerabilities Traded in Legal Markets*, *Reported Unpatched Vulnerabilities* and *Patched Vulnerabilities*. Our previous concept models (Radianti & Gonzalez, 2007), incorporated *Vulnerabilities Traded in Black Markets* in the vulnerability chain structure. We

did not find evidence of direct vulnerability trading in black market as described by Naraine (Naraine 2006) when a hacker sold exploits of WMF (Windows Meta File) flaw for US$4,000 underground. Nevertheless, all interviewees in this research agree that black market transactions occur. Most advertised tools in the black market observation were exploits and malware. Thus, the *Vulnerabilities Traded in Black Markets* was removed from the vulnerability chain structure and modeled as a separate sector (*see* Vulnerability Black Market Sector in section 4.3).

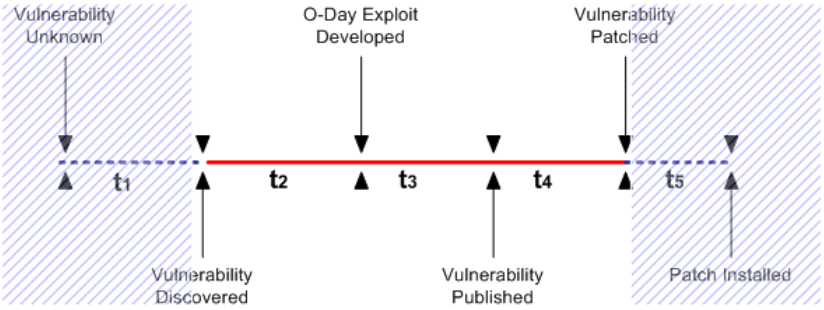

Figure 7
Vulnerability Timeline

The flows of vulnerability chains follow the common knowledge about vulnerability life cycles (Schneier 2000, Arora et.al 2006, Ozment 2005) and timelines from the discovery until the vulnerability patched, as portrayed in Figure 7. We did not investigate t_1, since far too little data are available. The time t_2 between discovery and 0-day exploit creation varies, but the shortest is 0-1 day. The next, t_3 can be a danger zone if the exploits are used for attacking victims. Together t_2 and t_3 can represent the process of reporting and coordinating with affected vendors which can take from one to twelve months before an announcement is made. In a few cases, it would take more than a year. The t_4 is a period between the vulnerability announcements and patched. On average, it took 21-66 days. The t_5 deals with patch installment and patch management, which is outside of the scope of this paper.

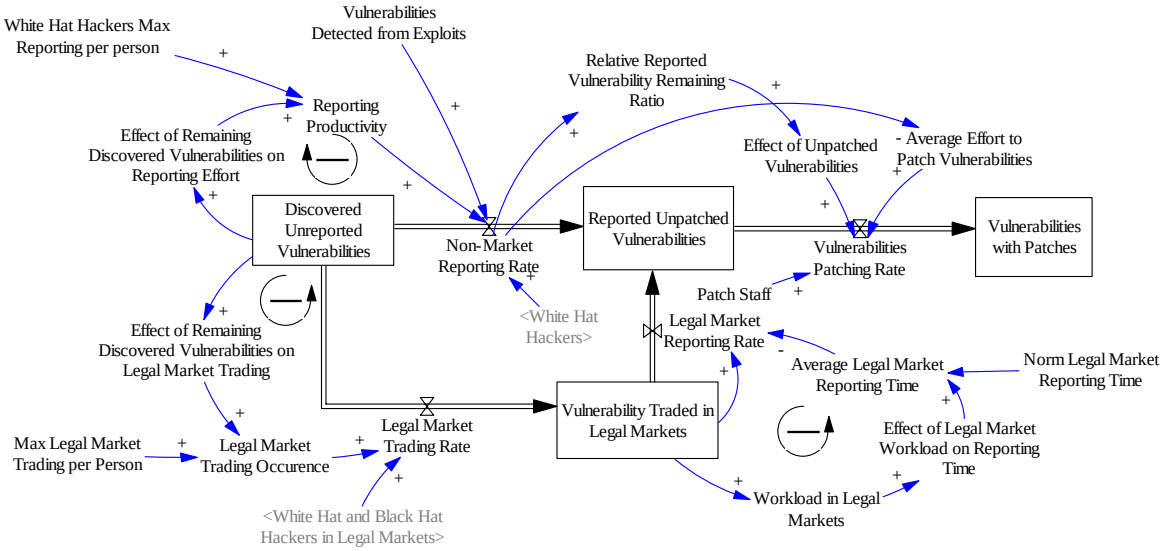

Figure 8
The Vulnerability Chain Sector

Discovered Unreported Vulnerabilities (Figure 8) are secret or non-published vulnerabilities. They have been discovered by various agents (internal discovery by security

companies and vendors, government discovery, BH and WH researchers) but have not yet been reported or announced. They become a restricted knowledge. *Reported Unpatched Vulnerabilities* are vulnerabilities that have been announced. Two inflows accumulate in *Reported Unpatched Vulnerabilities* stock—*Legal Market Reporting Rate* and *Non-Market Reporting Rate.* The former inflow is affected by three factors: White *Hat Hackers, Reporting Productivity* and *Vulnerabilities Detected from Exploits*. The outflow *Vulnerability Patching Rate* drains the stock. To assess a fraction of vulnerabilities detected from exploits, we searched vulnerabilities with "discovered in the wild" status in OSVDB database. In 2008, for example, there were seventeen vulnerabilities detected from exploits in the wild, or approximately 0.2 percent (0.002) of total reported vulnerabilities in a given year.

Legal Market Trading Rate links *Discovered Unreported Vulnerabilities* and *Vulnerabilities Traded in Legal Markets*. This captures today's development of the legal business model for software vulnerabilities. *Vulnerabilities Traded in Legal Market* refers to vulnerabilities that have already been acquired and bought by legal markets but have not yet been announced or published. The stock will also deplete when the vulnerabilities are announced. *Legal Market Reporting Rate* reflects this situation, and the report rapidity depends on *Average Legal Market Reporting Time*. This reporting time will be longer if *Workload in Legal Market* increases, e.g. too high burden to verify submitted vulnerabilities; no response from the affected vendors.

To model a legal market discovery, we follow the timeline of the disclosure stages in legal markets. Processing vulnerabilities in the legal market is shown in Figure 9 (similar processes as in Figure 8 occur before t_1 and after t_3; they are outside of the scope of our paper):

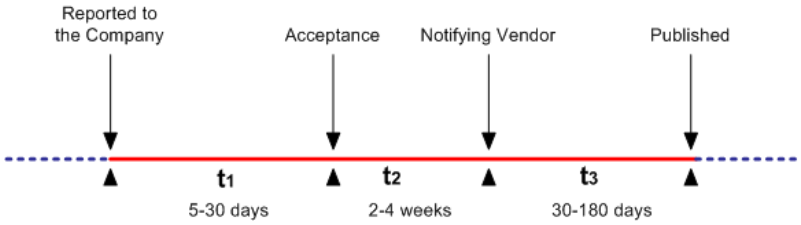

Figure 9
Legal Market Timeline

In timeline t_1 the company verifies the vulnerability or exploit. The verification length depends on a number of factors, such as the current queue of vulnerability submissions or the complexity of verification[7]. There are different practices among companies during t_2. TippingPoint for example, keeps secret a vulnerability discovery until a product vendor can develop a patch. During t_2, the subscribers only have a generic description of the protection service until the vulnerability is announced. Prior to announcement, the company may also circulate notification of the bought vulnerability to other security vendors. In the Vulnerability Contributor Program (VCP) case, after acquiring and verifying the vulnerability, the company notify vendor and the company's clients simultaneously. In most cases, the notification is sent to the vendor first, and then to the clients. During t_3 the company distributes an IPS (Intrusion Prevention System) to the subscribers and notifies the affected vendor. It may also coordinate public disclosure through a security advisory once a patch is ready. It is uncertain how long it takes vendors to react after notification. From the

[7] EAP (Exploit Acquisition Program) is an example vulnerability market practice that was shut down (March 2008), because of inability to complete a single transaction within the timeline (one month). In practice, the complete transaction took 4-7 months. Thus, the vulnerability was quietly patched and vulnerability value was gone.

timeline history in a VCP advisory, for example, we found some vendors responded very late—after public disclosure.

At the end of the vulnerability chain, *Reported Unpatched Vulnerabilities* flow to the *Vulnerabilities with Patches*. We assume that the last stock covers a range of solutions of software vulnerabilities such as patch, workaround, upgrade, discontinue the product, change default setting and third party solution. IBM (2009) finds that at the end of 2008, fifty-three percent of all vulnerabilities disclosed during the year had no vendor-supplied patches available to correct the vulnerability. And not all vendors go back to patch a previous year's vulnerabilities. The report states that forty-six percent and forty-four percent vulnerabilities from 2006 and 2007 respectively have no patch available at the end of 2008 (cf. OSVDB data on the number of patches in 2002-2008 in section 3.2). Below we summarize the parameters used in this sub model:

Table 5
Parameters in Vulnerability Chain Sector

Name of Parameter	Value, Unit
Initial Discovered Vulnerabilities	88,032 Vulns
Initial Reported Unpatched Vulnerabilities	212 Vulns
Initial Patched Vulnerabilities	1 Vulns
Initial Vulnerabilities in LM	0 Vulns
Max LM Trading per Person	0.05 Vulns/(Person*Month)
Max WH Reporting per person	0.6 Vulns/(Person*Month)
Normal LM Reporting Time	1.3 Months

4.2.2 Exploits Sector

There are three states of exploits: *Zero Day*, *Known* and *Patched Exploits*. The Exploits and Vulnerability sectors are modeled as a co-flow (Figure 10). The stock of *Zero Day Exploits* is an accumulation of exploits created from zero day vulnerabilities—privately known vulnerabilities. IBM (2008) finds independent researchers own around two percent of all exploits in pre-disclosure time. When they are revealed, *Zero Day* becomes *Known Exploits*, and when the vulnerabilities from *Known Exploits* are patched, the Exploits in principle are outdated becoming *Patched Exploits*.

Although some exploits become out of date because the vulnerabilities are patched, malicious actors may take advantages of the end user's negligence of not installing the patches immediately and when the window of vulnerability is still open. Arora et al.'s study (2006) shows that on average both *secret* and *published* vulnerabilities attract fewer attacks than *patched* vulnerabilities. Patching *known vulnerability* decreases the number of attacks, although initially attacks gradually increase over time after patch release. On contrary, patching an *unknown vulnerability* causes a spike in attacks, which then gradually decline after patch release. Attacks on secret vulnerabilities slowly increase over time until vulnerabilities are published and then attacks rapidly decrease with time after publication (ibid, 2006). A recent trend shows that 89 percent public exploits were released on the same day or before official vulnerability disclosure (IBM 2009), while in previous years it took weeks or months to create exploits after disclosure.

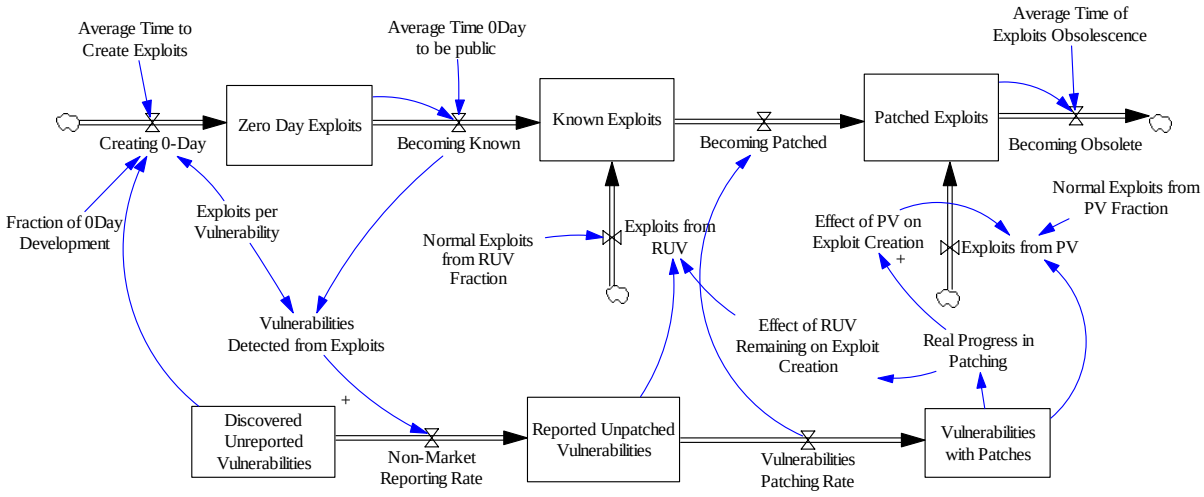

Figure 10
Exploits Sub Model

The foregoing information reveals that exploits will increase as the vulnerabilities are published. It is also in line with our observation that some exploits traded on black markets (Radianti and Ulltveit-Moe 2008) actually abused *published vulnerabilities* or *reported unpatched vulnerabilities* and were therefore included in our model. Two inflows affect the accumulation of *Known Exploits* in our model—*Becoming Known*, when the *Zero Day Exploits* become a public knowledge and *Exploits from RUV (Reported Unpatched Vulnerabilities)*, when new exploits are created from known vulnerabilities. IBM (2008) calls this a "public exploit" i.e. any proof-of-concept, demonstrative code, partially of fully functional or malicious mobile agent such as malware that is publicly available. *Patched Exploits* accumulates through inflow *Becoming Patched*—exploits that become outdated after the vulnerabilities have been patched and *Exploits from PV (Patched Vulnerabilities)*—newly created exploits after vulnerability fixed. A feedback from *Vulnerabilities Patching Rate* influences variable *Becoming Patched*. *Patched Exploits* will drain through outflow *Becoming Obsolete*. IBM (2008)) reports that the most common browser exploits in the first half of 2008 were one or two years old and that most of them were from 2006 and that patches for them had been available for some time. Arora et al. (2006) also indicates that nine percent of patched vulnerabilities are exploited.

Browne et al. (2000) found that the total number of exploits increases roughly as a square root of time since disclosure. Average time from discovery to leak (disclosure) is in the order of a month (Rescorla 2005). Furthermore, Arora et al. (2006) augmented the vulnerabilities data from CVE ICAT Database with data about the availability of exploit code. They divide various vulnerabilities—in protocols, operating systems, servers, applications, security products, open sources, freeware, as well as vulnerabilities that do not have a patch, secret vulnerabilities, published vulnerabilities and patched vulnerabilities—into *proportion exploited* and *unexploited*. Their findings show that the proportion exploited in secret vulnerabilities is 28%, in published vulnerabilities is 22% and in patched vulnerabilities 9%. It is possible that a single vulnerability induces multiple exploits. However, in the basic model, we assume there is only one exploit per vulnerability.

Table 6
Parameters in Vulnerability Chain Sub Model

Name of Parameter	Value
Average Time 0Day to be public	1 Months
Average Time of Exploits Obsolescence	2.5 Months
Average Time to Create Exploits	1 Months
Exploit per Vulnerability	1 Exploit per Vulnerability
Fraction of 0Day Development	28%
Normal Exploits from RUV Fraction	22%
Normal Exploits from PV Fraction	9%

4.2.3. Vulnerability Black Market Exploit Supply-Demand Sector

Exploit Sectors affects Vulnerability Black Market Exploit Supply-Demand Sector through a Total *Valuable Exploits* i.e., the sum of the rate of *Exploits from PV, Exploits from RUV* and *Creating 0-Day*. We modeled the market as a supply and demand of exploits, and this sub-model structure is created as order-response form. *Exploits in Black Markets* stock rises when there is an inflow from *Exploits Advertised in Black Market* and depletes because exploits are outdated (Figure 11). The inflow is determined by *Exploit Developed for BM* (Black Markets) and *Black Market Staffs*. The former variable depends on black hat hackers who participate in black markets and *Total Valuable Exploits* that can be advertised in black markets, while the latter variable captures a verification process by owner/staffs in black markets that determines the approval of the advertised commodities[8]. Exploits are out-of-date from black markets when exploits are sold and affected vulnerabilities are patched.

To keep black market attractive to the participants, after the exploits are outdated, an owner of a black market forum should ascertain a number of commodities are available. This is captured by *Expected Exploit Availability*. *Exploit Availability Gap*—a discrepancy between *Expected Exploit Availability* and *Exploits in Black Market*, pushes *Expected Exploit Advertising in BM* and furthermore influences the *Expected Staff to Verify Exploits*.

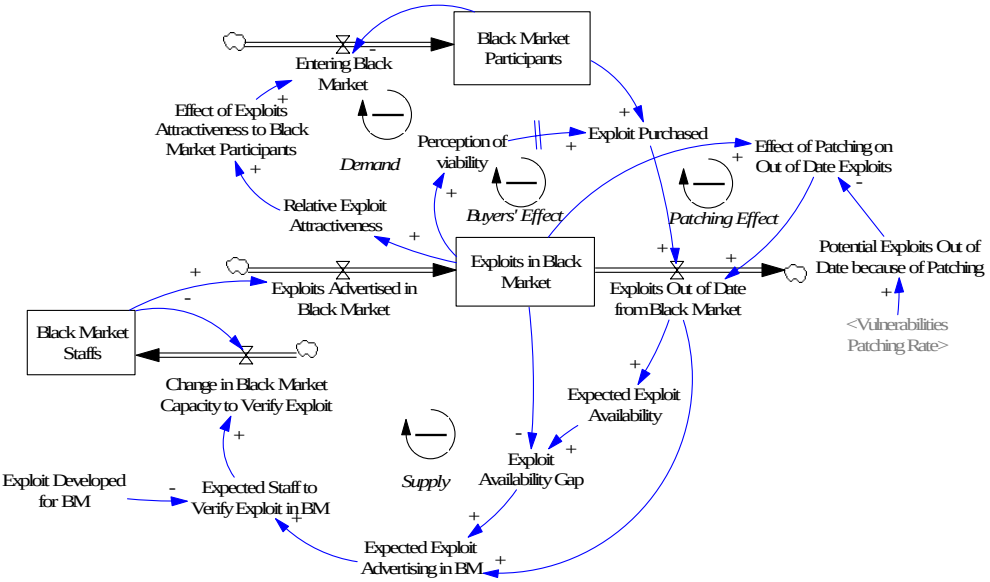

Figure 11
Exploit Supply-Demand Sub Model

[8] The knowledge about verification procedure is derived from our observation on several online black market forums (April 2006-May 2008).

It is very likely that the proliferation of exploits in BMs will result in more zero day attacks and that they will eventually leak to the public (IntelliSIGHT 2009), but our model does not capture further consequences or the possible usage of these exploits.

Table 7
Parameters in Vulnerability Chain Sub Model

Name of Parameter	Value
Exploit BM Demand per Person	1 Exploit/Person/Month
Exploit Duration in BM	3 Months
Time to Change Capacity	12 Months
Time to Close the Gap	0.5 Months

4.2.4 Security Researchers Sector

The security researchers or hackers sector provides input to the vulnerability chain sector. It is not a simple task to strictly divide the security researchers based on their "hat", e.g. black and white. The shifting meaning of "Hackers" as experts at programming and solving problems with a computer, leads people to begin color-coding them into white, black or grey hats to separate hackers into good, bad and something in between (Leung 2005; Parker 2005). Crume (2000) classifies hackers by their skill level, from *novice* (limited knowledge, bottom line of the hacker pyramid) and *intermediate* to *elite* (very skilful, capable of penetrating any system and creating new exploits). However, there is a strong suspicion bordering on certainty that some hackers are "white hat" security professionals who unravel new vulnerabilities as a part of their daily work.

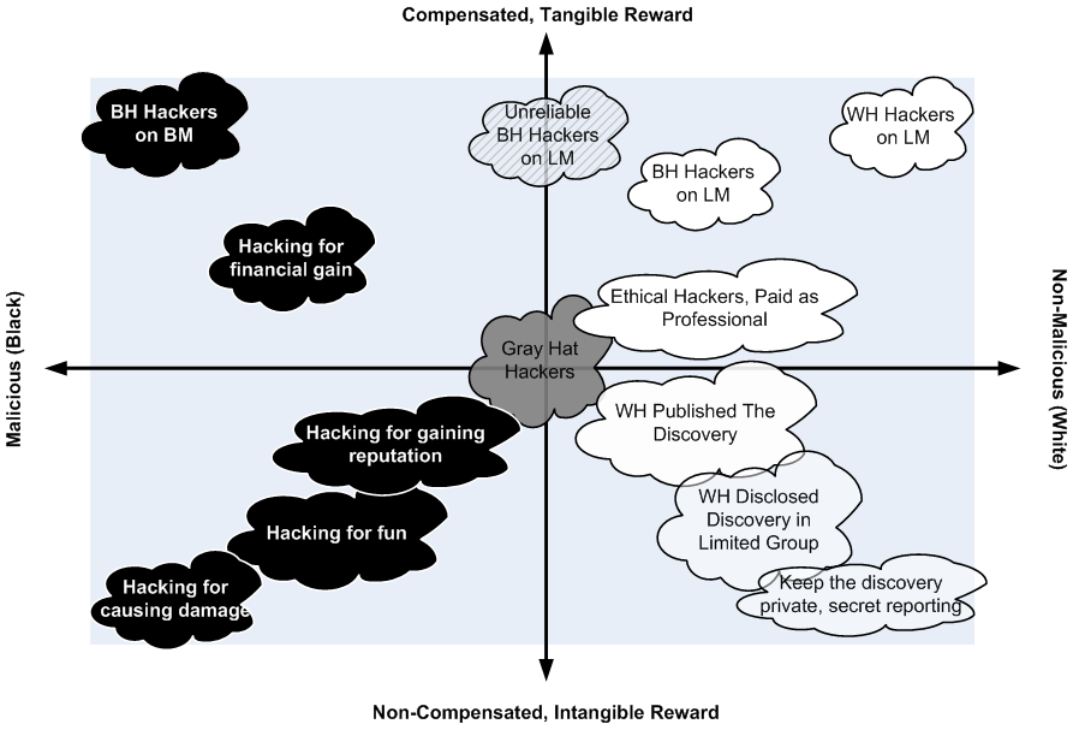

Figure 12
Black (BH), Gray and White Hat (WH) Hackers

For the purpose of our model, we need to be clear about the division of hackers since the vulnerability discovery process may involve both malicious and financial gain motive or altruistic-voluntary spirit. Concerning financial gain, we also encounter the division between

rewards obtained legally or illegally. In addition, some security researchers may act in legal markets while others may be hackers in underground and participating in black markets. Some of them may operate in both legal and black markets, or completely uncompensated hackers. Confusion also occurs when it comes to the legal-black market boundary. Miller (2007) points out EAP (a vulnerability market launched in 2007 and shutdown in March 2008) as a legal market since it announced openly. We had a short email interview with the program owner who suggested to "stay away from black markets, and legal markets are always better than black markets"[9]. However, an underground activist referred EAP as an "underground market". The following quotation of underground actor's email communication points up the aforementioned confusion:

> "I don't have experience selling to underground, I have just sold to ZDI and iDefense a few bugs because the offer was already fine...but it is hard to trust underground buyers so [I] never test for now. I think it is an advantage [because] you win money and you have things to put in [your] resume when you are entry level in the industry. But I do not see [any] big advantages. For selling underground I just know ["ATD@email"] who said he can buy my bugs [for] more than ZDI does, but I have never tried it. [It is] difficult to trust anyone in this field[10]".

Beyond such insights that there is a vague border between black and legal market, between black and white hat hacker, there is another important consideration for hackers on legal and black markets beside payment i.e. *trust*. That legal vulnerability trading might also attract security researchers was confirmed by CM: "Sadly I think it will reduce the security overall because individuals who currently practice "responsible" disclosure will begin to use the venue...[11]" Different categories of hackers in connection with the different motives, is illustrated in Figure 12.

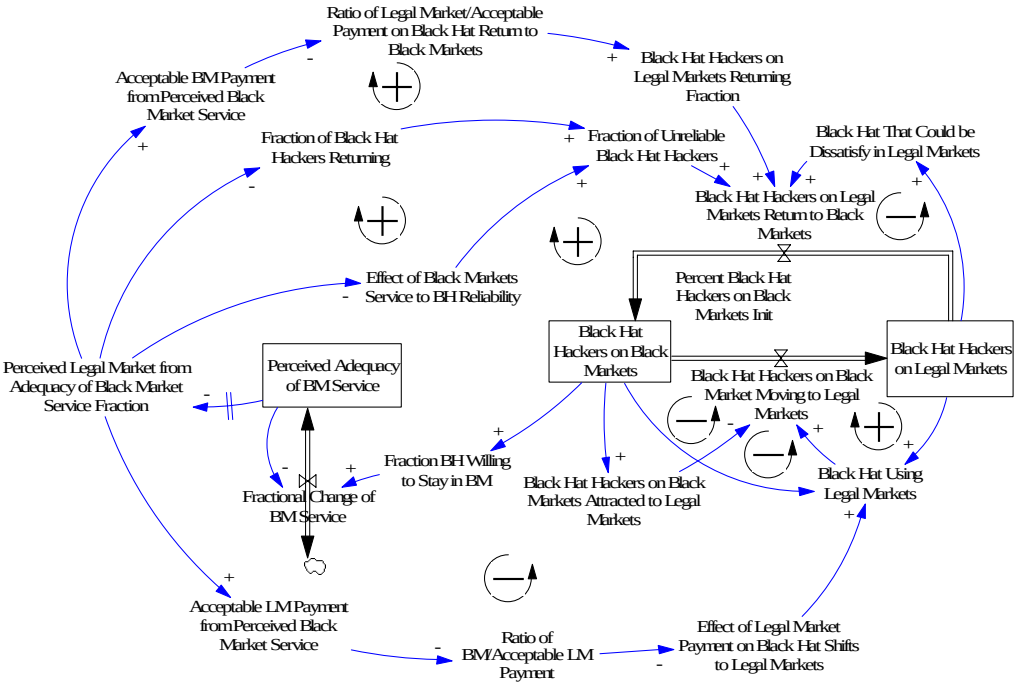

Figure 13
Black Hat Hacker Movements

The importance of security researchers sector in our model is that most of the non-compensated discovery activities depend heavily on white and black hat hacker's willingness to report or to submit their findings to both legal and black markets. We build two parallel

[9] Email interview, 16 May, 2007 with ATD
[10] Source: conversation via Private Message (PM) with administrator in Forum W9, July 8, 2008.
[11] Email interview with CM, May 18, 2007.

structures of black and white hackers and each is contains two stocks: *Black Hat Hackers on Black Markets* and *Black Hat Hackers on Legal Markets*, *White Hat Hackers on Legal Markets* and *White Hat Hackers* (Figures 13 and 14).

A *Black Hat Hacker on Black Market* is a researcher who is interested in a wide range of underground activities, ranging from creating and trading malicious tools and viruses, to exploits and perhaps vulnerabilities. A *Black Hat Hacker on Legal Market* is a researcher who moves into a legal market for financial incentives[12]. It is possible that *Black Hat Hacker on Legal Market* will return to black market. For example, one of our underground interviewees said to have a contact with a legal market and considered it is not relevant for his activities.

A *White Hat* is a researcher who notifies affected vendors when vulnerabilities are silently or openly discovered. To publish vulnerabilities is mostly driven by altruistic intentions and less by commercial motives. A *White Hat*'s ultimate goals are to push affected vendors to fix faster as well as improve software quality, and to warn end-users about the potential hazard caused by the discovered vulnerabilities. A *White Hat* might also be attracted to the legal market program and move into legal market. This group is categorized as *White Hat on Legal Markets*. There are two ways for migration of white hats to legal markets: they actively join to markets or security companies recruit them. VCP, for example, using Las Vegas Black Hat Conference each year, host a recruitment party[13]. There is also reason to believe that a few researchers will stay "white" and reluctant to deal with black markets for legal grounds. CM specified aforementioned issue that in legal markets:"…if someone (a company) likes TippingPoint[14] screws you, you can yell and scream and hurt their business. On the black market there is nothing you can do...[15]" Sometimes, the security company ultimately hires a few of them to be permanent researchers.

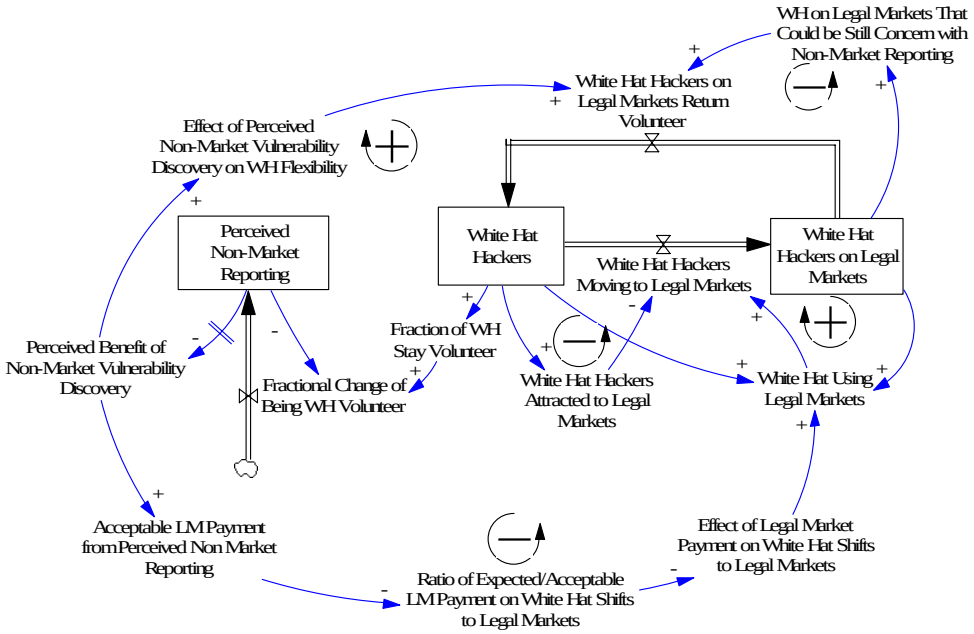

Figure 14
White Hat Hacker Movement

[12] However, legal markets, such as VCP, prefer not to investigate if their researchers have acted in the underground. There are no ways to verify this status and such action will breach the trust between the company and contributors (Email interview, 9 June 2009).
[13] Email interview on June 3, 2009 with director of iDefense Vulnerability R&D Attack Labs
[14] The interviewee talked about TippingPoint Security Company, see http://www.tippingpoint.com/
[15] Email interview on May 18, 2007 with CM .

There are a few concerns with the market approach development that may induce security researchers to sell vulnerabilities to multiple agents (legal or underground market). CM commented that such concerns are real, since "... [The] economic incentive is too high and since these guys are dealing with criminals, it is unreasonable to assume that they will be true to their word to only sell to one person..."[16] The flow returns from black hat in legal market to black hat in black market capture the possibility when black hat is becoming unreliable and still deals with black market.

In short, there are some loops/ factors affecting the dynamics of hackers in black markets and legal markets. So far our model accommodates the payment in black market as driving factors of the black and white hat hacker movement.

Regarding the number of hackers, one author estimates that there are around 100,000 "clueless" hackers, 5,000 skilled intermediates hackers, and 500-1,000 skillful hackers worldwide (Crume 2000, p.25). OSVDB in June 2007 credited at least 3,267 contributors who reported vulnerabilities. In legal markets, VCP in early 2009 claimed to cooperate with 250 researchers while ZDI cited to have 925 registered researchers, or increased around 6.7 percent since July 2008 statistics (there were 860 researchers).

Our observation in three black market forums on active members (April 2006- June 2008), we found 315, 338 and 515 unique names of underground hackers in forum W1, W2 and W6[17] respectively. Certainly, there was an overlap among these numbers as we noticed that many participants entered multiple forums using a single pseudonym. Likewise in legal market, a few researchers might be registered either in VCP or ZDI. And the contributors in OSVDB might originate from these companies. We even recognized a contributor registered by OSVDB as a staff in forum W2, since he uses the same black market pseudonym. We select 5,000 as the initial value of hackers and distribute them accordingly:

Table 8
Parameters in Security Researchers Sub Model

Name of Parameter	Value
Hackers	5000 persons
Percent Black Hat Hackers on Black Markets Init	10 %
Percent Black Hat Hackers on Legal Markets Init	0 %
Percent White Hat Hackers Init	70 %
Percent White Hat Hackers on Legal Markets Init	20 %

4.2.5 Payment Sector

Remember in section 4.2.4, payment sector is a driving factor that attracts white hat and black hat hacker to be in legal market or black market. In the model we assume that hackers will stay in black or legal market, depend upon the motivation and satisfaction from the obtained reward. Amount of payment in legal markets varies and is not so transparent. VCP e.g., rewards as much as $15,000 (US), depending on the nature of the vulnerabilities documentation and reliable *proof-of-concept* exploit code. However, the actual payments for the researchers are obscure.

We only know the potential income generated from black market based on the advertised price per malicious tool. So far, the price of various exploits range from US$500 to 1,500. However, a seller could expect a higher income from multiple transactions. Two black market sellers mentioned two different ranges of income in an online interview[18]. One claimed to earn around US$ 500, another mentioned to earn around US$ 10,000 a month.

[16] Email Interview with CM, May 2007
[17] We coded the observed BM Forums as W1, W2…W12
[18] Online interview with vv and zz, 26 January 2009

Due to the uncertainty with the exact amount of income from both markets, we set an equal parameter value for either *Payment per Legal Market* or *per Black Market*, i.e. US $1,000. Figure 15 shows the payment sector on black market. We have a similar payment structure for white hat hacker.

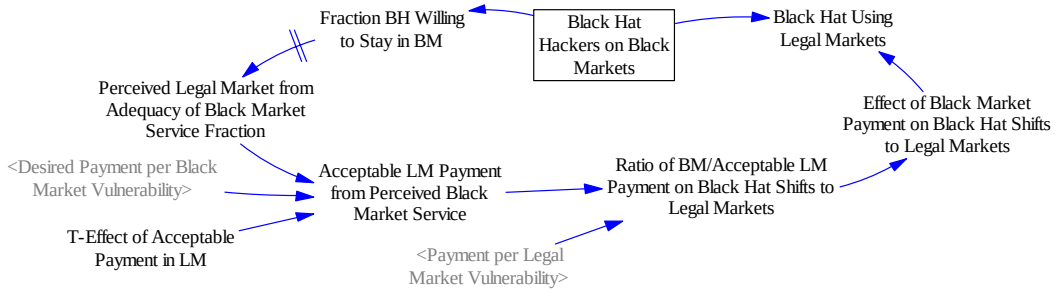

Figure 15
Payment Sector

A security researcher who had experiences with trading bugs on legal markets shared the experience in an underground forum. One legal market deemed as providing good payment for critical vulnerabilities had a friendly staff and fast payment. However, there are minor criticisms that the company refuses many bugs, and it would ask for a refund if the discovered vulnerabilities were patched, even though the company had acquired the bugs before patching. Another legal market was evaluated as good because it accepted many bugs. However, the payment was judged as low (without mentioning the amount) and the researcher was uncomfortable with the submission procedure.[19]

5. Model Validation and Simulation

5.1 Validation

Model adequacy needs to consider its purpose. Therefore, Forrester reminds modelers that adequacy does not mean proof of validity. There is no way to prove validity of a theory that purports to represent behavior in the real world; one can achieve only different degrees of confidence in the model (Forrester 1994). Validity of a model depends on its suitability for a particular purpose (Forrester 1961). Thus, judging the utility of a model should include its purpose, which is essentially a non-technical, informal, qualitative process (Barlas 1996). Basically, validation occurs in every stage of the modeling, but Barlas emphasizes the importance of conducting formal validation before simulation. Sterman (2000) suggests 12 formal tests to validate the model

Using Vensim we performed several tests such as dimensional consistency test and sensitivity test. A few simulations were implemented to test the suitability of the time step (0.125) and integration method. To perform a parameter confirmation test, we searched the literature for an available knowledge about the real system, including statistical data. For parameters which we did not have empirical values we used a "best guess" approximation, tested the value of our assumptions using Vensim's sensitivity analysis, and adjusted the parameters to replicate the time series data, as in Figures 1a and 1b (see Section 3.2).

Figures 16 and 17 show a model behavior as a replication of the reference mode showing the development of *Reported Unpatched Vulnerabilities* and *Vulnerabilities traded*

[19] Source: CL, Forum W9, Accessed May 20, 2008.

in LMs in the period 2002-2008 (see Section 3.2). To calibrate the model, we adjusted parameter values, using our best judgments rather than precise statistical estimates.

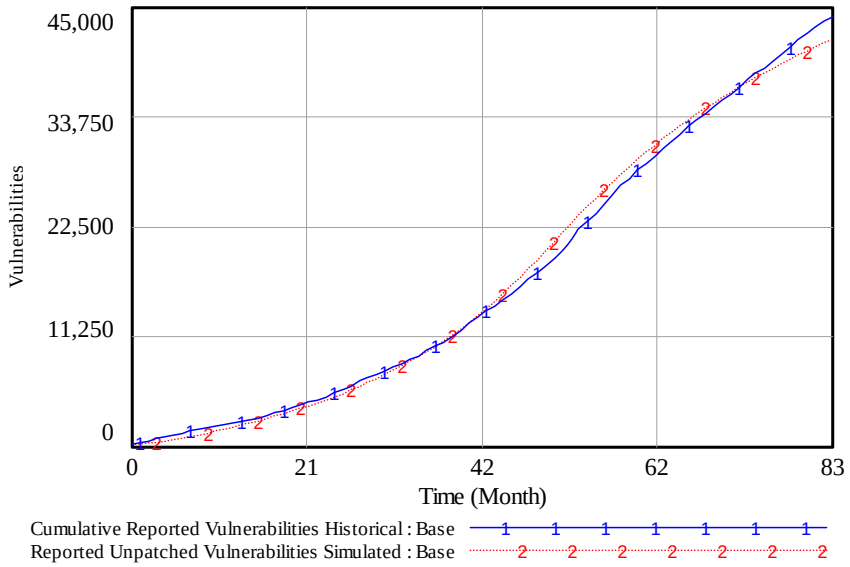

Figure 16
Historical vs. Simulated Reported Unpatched Vulnerabilities

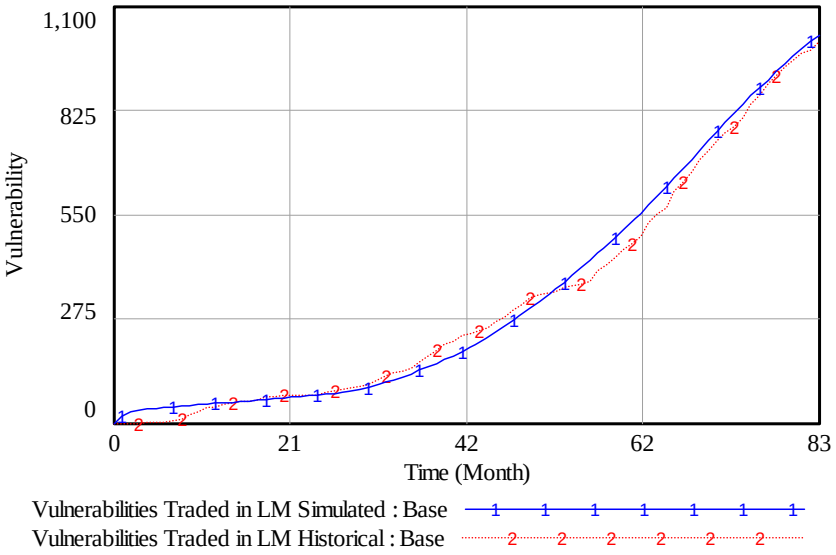

Figure 17
Historical vs. Simulated Vulnerabilities Traded in LM

Quantitative validation of a model is preferable when the data is available, but Forrester (Forrester 1961) and Barlas & Carpenter (1990) also stress the role of qualitative validation. If most of the coverage of a model is derived from non-quantitative forms such as verbal and written descriptions or human experience and knowledge, a sound model need to be validated from the same kind of knowledge. Several parts of this black market model were drawn from non-numerical sources. Hence, a qualitative validation is required, but this process has not yet been completed.

5.2. Simulation

5.2.1 Base Case

A set of assumptions were made in formulating our vulnerability black market model. The model begins with discovered unreported vulnerabilities, i.e. those discovered but not yet announced by vendors or vulnerability reporting coordinators. Thus, we did not consider any unknown vulnerabilities, since they are too difficult to assess. We also look at discovered vulnerabilities as an aggregate, and do not regard flaws in a specific product (e.g. Microsoft, etc). We assume that any vulnerability is equally harmful and bears the risk of being exploited by malicious actors. In addition, the model does not consider the risk of being punished when hackers entering black market and selling exploits.

There are two kinds of vulnerability disclosure—vulnerabilities disclosed simultaneously with patches to reduce the window of exposure; and, one in which patches are developed after the vulnerabilities have been published. We assume that the discovery timeline follows the second disclosure type. This assumption makes sense, as we found that only a small number of the vulnerabilities had actually been fixed. In the base case, only white hat hackers are moving to legal markets and no one returns voluntarily after involving on legal markets. In the beginning, the stock of black hat hackers stays constant and no one moves to legal markets. Thus, black hat hackers do not yet affect the change in the stock of vulnerabilities in legal markets, and only influence Black Market Supply Demand Sector.

Figure 18 shows a few initial behaviors of the vulnerabilities in various phases. In early stage of simulation, *Reported Unpatched Vulnerabilities*, *Vulnerabilities Traded in Legal Markets* and *Patched Vulnerabilities* grow together. Because the low initial patching staff and limited patching effort create slower patching rate, the accumulation *Reported Unpatched Vulnerabilities* are greater than the accumulation of *Patched Vulnerabilities* during these simulation time frame. Hence, a lot of vulnerabilities are unsolved. On the other hand, the *Vulnerability Traded in Legal Markets* begins to grow, as a number of white hat hackers are moving into legal markets (Figure 19). Thus, the legal markets are assumed to successfully attract white hat hackers through their payment program. *Vulnerabilities Traded in legal market* is growing a bit fast between months 84-132, before it declines. The possible explanations for this rapid growth are combinations either higher inflow of vulnerabilities traded in legal markets or slower outflow of legal market reporting rate. Our model assumes that greater vulnerability acquisitions lead into longer time to report. This assumption is grounded from the calculation of the historical record on average reporting time in VCP that shows increasing time. In 2002, on average it took 29 days from a vulnerability acquisition to publication—47 days in 2003, 50 days in 2004, 65 days in 2005, and 119 days in 2006. A declining trend in simulation occurs between months 122 to 168 because of fewer legal market discoveries. Our model assumes a fixed initial number of discovered (secret) vulnerabilities. Thus, near the end of simulation, the fraction of the discovered vulnerabilities compared to the initial value is getting smaller and slows-down vulnerability reporting and trading activities.

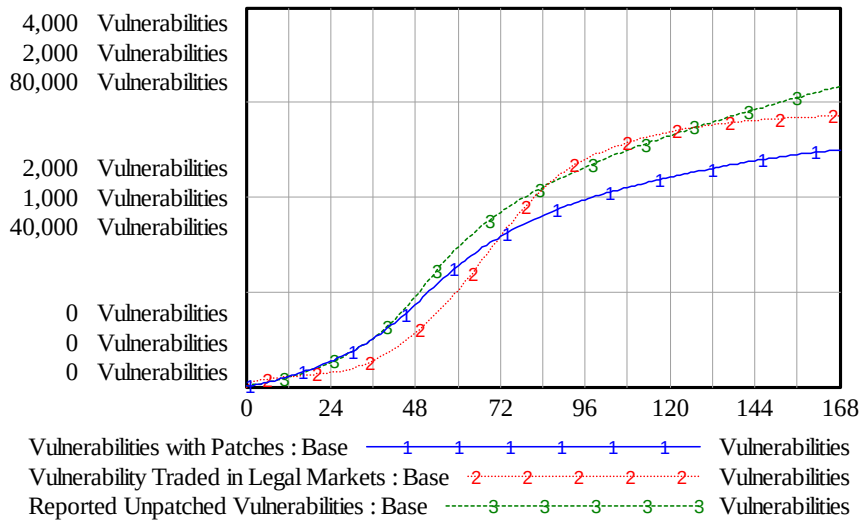

Figure 18
Simulation of Vulnerabilities

The security researchers' sector is responsible for most of the stock changes in the vulnerability chain sector. Figure 19 shows the base run simulation of hackers. Line 5 shows the number of hackers, i.e. 5,000 persons. We assume that no black hat hackers move to legal markets (Line 4). Thus, black hat hackers on black markets stay constant over time, i.e. 1,000 persons (Line 3). Black hat hackers so far only affect the exploit supply demand in black markets.

The stock of white hat hackers decreases (Line 1) as more of them shift on legal markets (Line 2). If the shifting trend continues, in the end of a simulation time most of white hat hackers would have experiences to involve in legal markets (around 95 percent of white hat hackers Initial). If we look at the Figure 18, the growth of *Reported Unpatched Vulnerabilities* slows down by month 60. It is a point where white hat hackers also move slower to legal markets and fewer white hat hackers stay voluntarily.

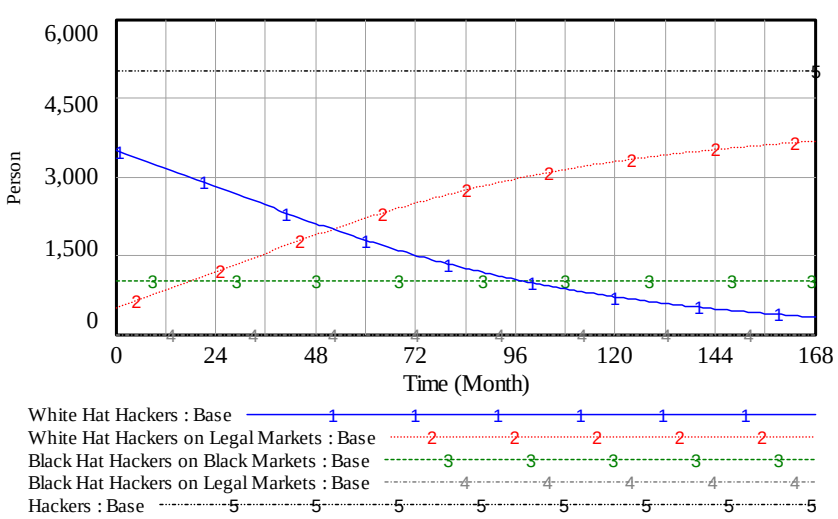

Figure 19
Simulation of Hackers

We also can notice the development of the proportion of legal market and non-legal market reporting to overall vulnerability discovery over time (Figure 20). A declining trend in

non-legal market reporting happens, as more vulnerabilities reported from legal markets, particularly after month 72. However, in the long-run, contributions from LM and non-LM reporting show flattening trends.

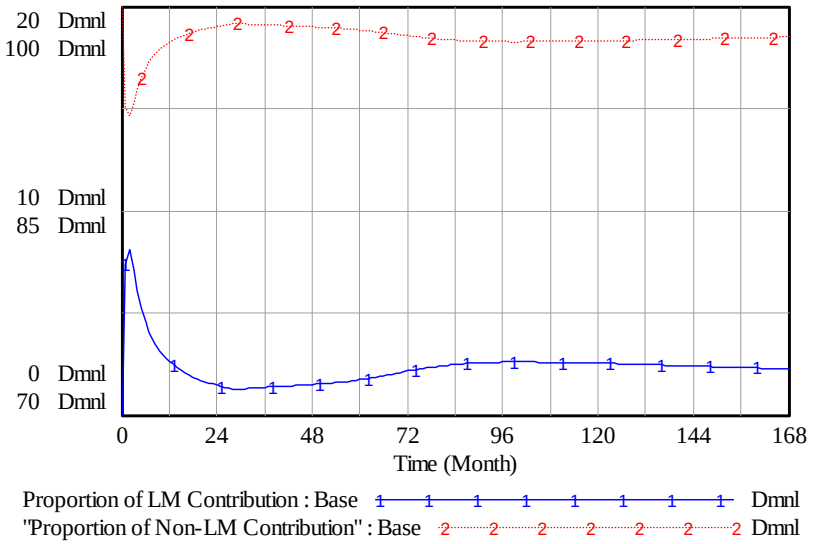

Figure 20
Proportion of Legal Market (LM) and Non-LM Reporting to Total Vulnerability Discovery

The dynamics of supply and demand of the black market for exploits can be seen in Figure 21. The exploits in black market shows relatively stable behavior, although exploit developed for black market (line 3) are increasing. The verification structure and exploits being outdated from black market are among explanations for producing such behavior. Under base scenario initial conditions, the model produces dynamic behaviors consistent with known behaviors observed in the case study.

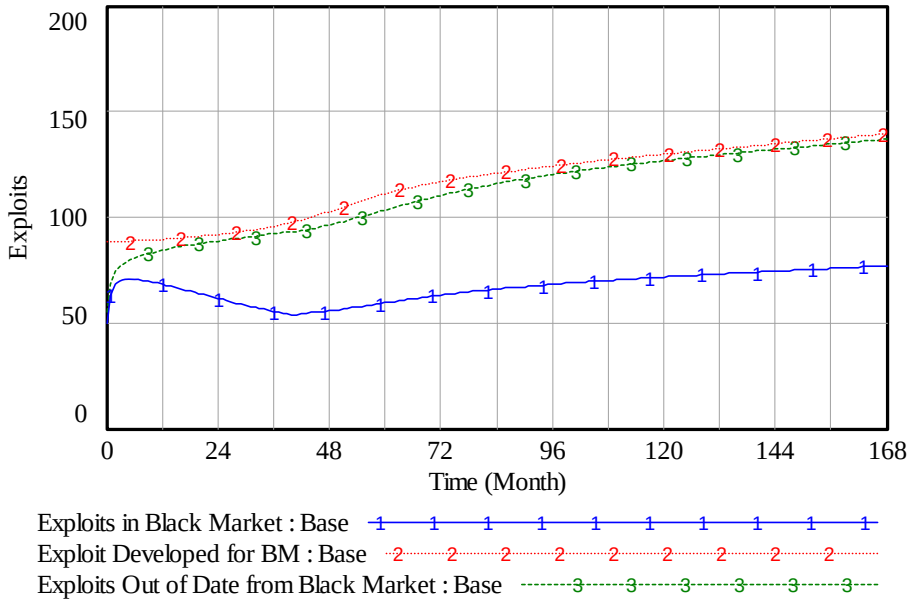

Figure 21
Exploit Developed for BM, Exploit Availability Gap, and Patched Vulnerabilities

To investigate how structural intervention may affect the system under study, we conduct a series of simulation using the model. We analyze the behaviors resulting from parameters and initial conditions different from those of the base case. In order to explore the efficiency of the market approach policy in promoting the vulnerability reporting and encountering the black market effect, three experiments are implemented. In the first experiment, we assume the vulnerability market is efficient, both black hat and white hat hackers are attracted in the payment program from legal markets.

In the second experiment, higher percentage of white hat hackers stay white, or return volunteer, and higher percentage of black hat hackers stay in black market and some of those who involved in legal markets also return to black markets. An incentive from black markets is higher than legal markets. In the third experiment, we keep the previous assumptions and add better patching mechanisms; the vendors are able to react faster.

5.2.2 Results

Figures 22, 23 and 24 show the behaviors of *Reported Unpatched Vulnerabilities*, *Vulnerabilities Traded in Legal Markets* and *Patched Vulnerabilities* in the three scenarios, and compare them to the base case. The first policy (BH Hackers Move to LM Scenario, Line 1) test shows that focusing on the legal markets does attract the black hat hackers, and more hackers join the program. However we also noticed that the number of reported unpatched vulnerabilities (Figure 22) is slightly higher accumulated than in the base run. This may be affected by the efficiency of legal markets (Figure 23) that are still able to fulfill the normal timeline schedule for announcing bought vulnerabilities--with or without patch available (about legal market timeline, see section 4.2.1). A slowdown trend in the three curves in Figure 22 occurs because of slower reporting activities, as many vulnerabilities are detected, compared to the initial value.

Vulnerabilities traded in legal markets (Figure 23) are a little bit lower in the second scenario (HiBM Payment, Line 2), where we put several assumptions i.e. higher expected income from black markets, black hat in legal market might return to black market or white hat hackers become volunteers and there are minimum number of white hat and black hat hackers stay in legal markets. These explain why in the second scenario, a lower number of vulnerabilities are traded in legal markets. Thus higher black market payment retards legal market activities since some hackers return to black markets. Under all three scenarios, the curves in Figure 23 flatten approximately after months 108. That happens because of the capability of legal markets to process the reporting mechanism. The more independent researchers report the vulnerabilities via market channel, the higher the workload of legal markets to verify them. It may take a longer time to organize and further conduct the normal reporting procedure as we described in the section 4. In the third scenario (Efficient Patching, Line 3) we noticed that more vulnerabilities are patched when we double the patch staff and increase the effort to patch. The curve of vulnerabilities traded in legal markets (Line 3) is higher than the second scenario—higher black market payment. White hat hackers are flexible to move between voluntary reporting and compensated discoveries and black hat hackers can evaluate the legal market and return to black market. The highest trading volume occurs in scenario 1 (Line 1) when either black or white hat hackers are attracted to the payment program.

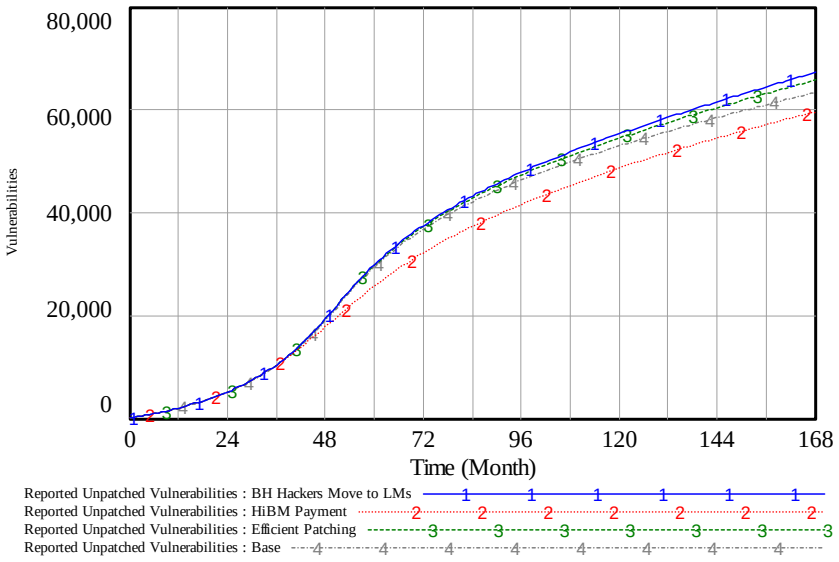

Figure 22
Simulation Result Reported Unpatched Vulnerabilities

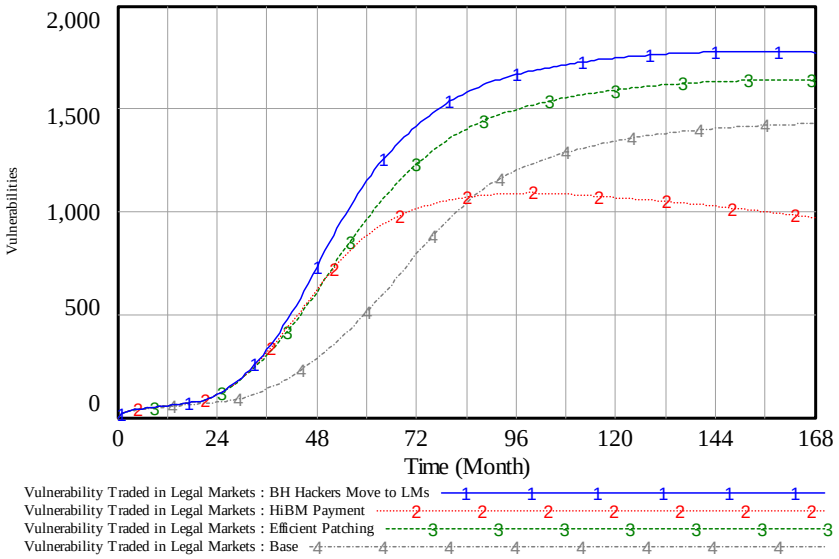

Figure 23
Simulation Results Vulnerabilities Traded in LMs

The third policy is to reorganize the patching procedure while we still maintain the assumptions in the second scenario. We can see the behavior of the main variables. The reported unpatched vulnerabilities are decreased, however, in line with some positive reaction in several parts of the system such as increasing patched vulnerabilities, decreasing trend of the vulnerability exploits and fewer hackers involved in black markets.

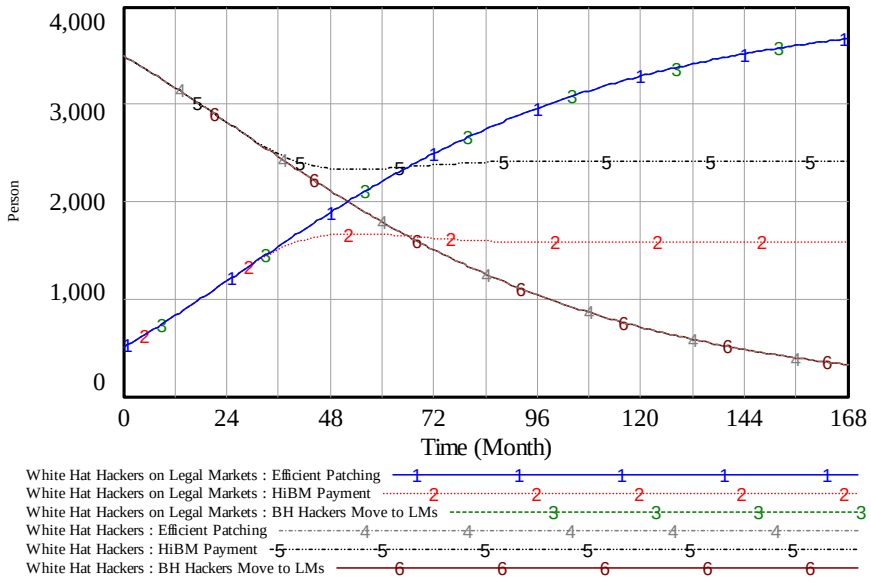

Figure 24
Simulation Results of White Hat Hackers

Figures 24 and 25 show the dynamics both white hat and black hat hackers. The first policy test shows that the number of black hat hackers in legal markets grows (note, the black hat hacker initial value is 1000). The second policy test shows that the actual payment and expected income from both markets start influencing the decision of the hackers to stay performing voluntary reporting or return to black markets. A higher number of hackers wants to stay in black market as well as higher expected income from black markets prevent hackers from moving to legal market. The second policy test also demonstrates an equal development of the black hat hackers in legal markets. In patching scenario (policy test 3) fewer black hat hackers move to legal markets.

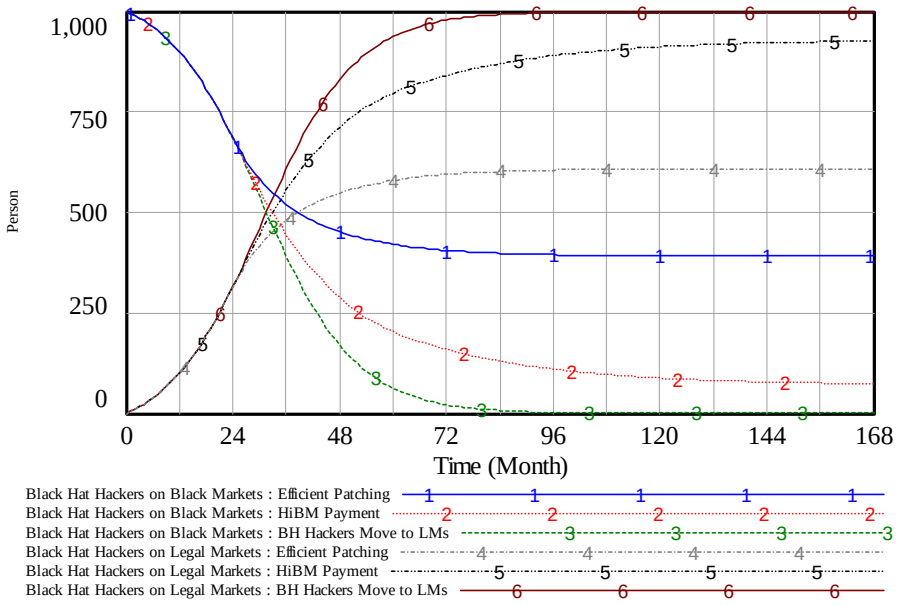

Figure 25
Simulation Results of Black Hat Hackers

On the other hand, under the three scenarios, white hat hackers are allowed to move to legal markets. Thus, if all researchers are interested in this payment program, we could see that the reported unpatched vulnerabilities are lower than the initial value. When we allow white hat hackers to be flexible, we could notice the differences where we have got smaller white hat hackers in legal markets.

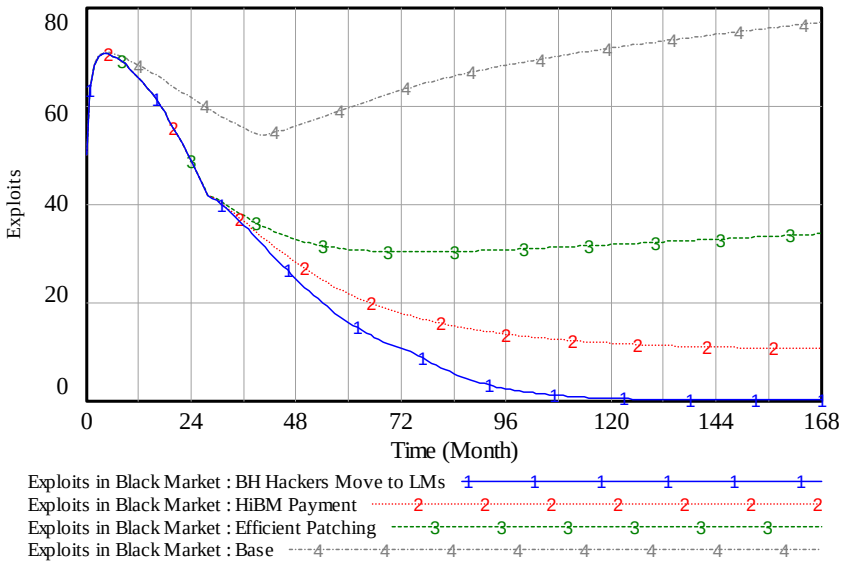

Figure 26
Simulation Results of Exploit for Black Market

We finally turn to the exploit supply and demand. We only show one simulation about the exploits developed by black hat hackers for black markets (Figure 26). The first policy test (Line 1) shows that the activities in black markets are less intensive as more hackers are attracted to enter legal markets. Since the simulation in this scenario assumes that payment is the only reason for hackers to move to legal market, the curve 3 falls to zero around month 132—a month where all black hat hackers in this scenario have shifted to legal markets. The second policy test (Curve 2) causes higher exploit creation for black markets, due to the higher expected income. But the curve is not as high as the base case (where all black hat hackers are in the black markets only). In the third policy test (Curve 3), the behavior is only slight different from Curve 2. Thus, efficient patching increase the number of patched vulnerabilities. But if the discoveries continue to grow, and vendors cannot react fast on facing the rapidity of the vulnerability reporting and announcement, an opportunity for black hat hackers to develop exploits is still open.

6. Conclusion

This paper attempts to answer several questions, such as what factors affect the success and the failure of the markets. The use of the system dynamics method is to help us to see different scenario and different impacts of them on main variables we wanted to observe.

Implication for the policy adoption in the field of vulnerability disclosure and vulnerability black markets:

Patching does not necessarily solve the vulnerability problem as long as users do not install patches or updates immediately. A chance for hackers to continue creating exploits and attack the ignorant users is still open. However we must admit that both patched and unpatched vulnerabilities introduce their individual risk. If the reported vulnerabilities are patched, a

small amount of hackers will still be dedicated to develop exploits. And the recent trend shows that the exploits are assembled into a kit so that users can easily use them as an attack tools using vulnerabilities with patches. However, the risks are not as high as the one driven from unpatched vulnerabilities. The simulations confirms that payment may be an attraction for hackers in order to submit their discovered bugs, but does not necessarily fasten the reporting process and the announcement, when in certain situations legal market workload exceed the capability to complete an individual transaction—and market will not be an efficient channel. EAP shutdown was an example where a vulnerability market has to proceed 7 months for a single transaction, longer than an initial plan to complete it within one month. As vulnerabilities are sensitive-to-time commodity, such longer processing time might erode the researchers' trust on the market (we have not yet modeled this issue).

Black Markets depend heavily upon the dynamics of the vulnerability discovery, channeling, and patching processes. It is a counterintuitive result that exploits still are possible to be developed in black markets when the vendor patches faster. Here, awareness of software end users is becoming more important.

Implication for Information Security (InfoSec) Research

InfoSec problems contain some feedbacks and non-linearity relationships among the causal factors. Most of security researches approaching this field using more technical methods including statistics and econometric modeling. Such approaches sometimes need more precise and statistical data; otherwise, there is no way to explain the problem. Complexities in InfoSec of problems need to be investigated in a comprehensive approach. SD focuses on the structure and behavior of systems composed of interacting feedback loops (Goodman 1974). Complexities, non-linearity, and feedbacks can be captured using this method. Numerical data are not the only base for modeling since information derived from the human knowledge, experience or observation, are another rich modeling sources. To combine SD with InfoSec research may provide broader insights. Some efforts in this field have been initiated, (for example, Gonzalez and Sawicka 2003; Rich et al. 2005; Dutta and Roy 2009). This research is a further example how SD and dynamic modeling contributes to InfoSec research.

Limitations

There are several limitations in this study. For example, we treated the vulnerability data as an aggregate, without trying to differentiate between the software product that has a very high market value and free software where the users or malicious agents are not interested in developing exploits for such software. In addition the vulnerability value of software product in vulnerability markets varies, and not only depends on severity and criticality of the flaws but also type of products affected by the vulnerabilities and how many people use such kind of software. Some legal markets may have a clear requirement, what kind of product they are interested in or otherwise they will reject the submitted bugs. We did not consider such differentiation and treat all vulnerabilities have equal value in the markets. Information on black market practice is obtained completely from the disguised observation. We also simplify black market commodities into "Exploit" while there are many type of malicious tool other than exploits traded black market e.g. malicious tools that could be used to steal confidential information or to help penetrate system. Such kind of targets reflects the vulnerability in the network system, rather than in the software as a result of a mistake in the programming phase. Some malicious tools even deal with the social vulnerabilities—tools taking advantage of human weakness or unfamiliarity with situations in the cyber space, and using these tools to exploit this weakness. Our assumption in the model follows disclose-and patch vulnerability timeline, and do not try to model the opposite sequence: patch and then

disclose the vulnerabilities. We evaluate the market-based discovery only from the quantity of their contribution to overall vulnerability discovery. Companies might have advance criteria, such as quality of the vulnerability research, severity of vulnerability findings and how to provide better protection to their subscribers.

Future Elaboration

A few tests and refinements are still required, without changing the main structure of the model, particularly the supply and demand in the black market. A few distinct features of the vulnerability black market make its supply and demand different from a price mediated market. The black market owner does not produce malicious code and does not decide how many malicious tools should be available in the market. The commodities are supplied by market participants. The refinements aim at ensuring that the black market supply and demand part has already captured the basic trait of the vulnerability black market.

Acknowledgment

The first author would like to thank to Richard Parr for his assistance in the development of this paper. The author is also grateful to numerous interviewees, and anonymous underground members who generously answered various questions during conducting this research.

References

Anderson, Ross. 2001. Why Information Security Is Hard, an Economic Perspective. Paper read at 17th Annual Computer Security Applications Conference.

Arbaugh, William. A., William. L. Fithen, and John McHugh. 2000. Windows of Vulnerability: A Case Study Analysis. *Computer* 33 (12):52-59.

Arora, Ashish, Ramayya Krishnan, Anand Nandkumar, Rahul Telang, and Yubao Yang. 2004. Impact of Vulnerability Disclosure and Patch Availability: an Empirical Analysis. Paper read at Workshop of Economics and Information Security (WEIS), at Minneapolis, MN.

Arora, Ashish, Anand Nandkumar, and Rahul Telang. 2006. Does Information Security Attack Frequency Increase With Vulnerability Disclosure? An Empirical Analysis. *Information System Frontiers* 8 (5):350-362.

Arora, Ashish, Rahul Telang, and Hao Xu. 2008. Optimal Policy for Software Vulnerability Disclosure. *Management Science* 54 (4):642-656.

Barlas, Yaman. 1996. Formal Aspects of Model Validity and Validation in System Dynamics. *System Dynamics Review* 12 (3):183-210.

Barlas, Yaman, and Stanley Carpenter. 1990. Philosophical Roots of Model Validation: Two Paradigms. *System Dynamics Review* 6 (2):148-166.

Boulding, Kenneth E. 1947. A Note on the Theory of the Black Market. *The Canadian Journal of Economics and Political Science / Revue Canadienne d'Economique et de Science Politique* 13 (1):115-118.

Bronfenbrenner, Martin. 1947. Price Control Under Imperfect Competition. *The American Economic Review* Vol. 37 (1):107-120.

Browne, Hilary. K., William. A. Arbaugh, John McHugh, and William. L. Fithen. 2000. A Trend Analysis of Exploitations. http://www.cs.umd.edu/~waa/pubs/CS-TR-4200.pdf.

Böhme, Rainer. 2006. A Comparison of Market Approaches to Software Vulnerability Disclosure. Paper read at Emerging Trends in Information and Communication Security (ETRICS) 2006 June 6-9, at Freiburg, Germany.

Cavusoglu, Hasan, Huseyin Cavusoglu, and Srinivasan Raghunathan. 2005. Emerging Issues in Responsible Vulnerability Disclosure. Paper read at 4th Workshop of Economic and Information Security (WEIS), at Cambridge, MA, USA.

Crume, Jeff. 2000. *Inside Internet Security*. Harlow, England: Addison-Wesley.

Du, Wenliang, and Aditya. P Mathur. 1998. Categorization of Software Errors that Led to Security Breaches Paper read at 21st National Information Systems Security Conference, at Crystal City, Virginia, VA.

Dutta, Amitava, and Rahul Roy. 2009. Dynamics of Organizational Information Security. *System Dynamics Review* 24 (3):349-375.

Engle, Sophie, Sean Whalen, Damien Howard, and Matt Bishop. 2006. Tree Approach to Vulnerability Classification. Davis, CA: Dept. of Computer Science, University of California at Davis.

Forrester, Jay W. 1961. *Industrial Dynamics*. Cambridge, Massachussets: The MIT Press.

———. 1994. System Dynamics, Systems Thinking, and Soft OR. *System Dynamics Review* 10 (2):245-256.

Franklin, Jason, Vern Paxson, Adrian Perrig, and Stefan Savage. 2007. An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants. Paper read at 14 th ACM Conference on Computer and Communications Security (CCS), at Alexandria, VA, USA.

Gonzalez, Jose J., and Agata Sawicka. 2003. The Role of Learning and Risk Perception in Compliance. Paper read at 21st International Conference of System Dynamics Society at New York City.

Goodman, Michael. 1974. *Study Notes in System Dynamics*. Cambridge, Massachusetts: Wright-Allen Press, Inc.

Gönensay, Emre 1966. The Theory of Black Market Prices. *Economica, New Series* 33 (160):219-225.

Higgins, Kelly Jackson. 2008. Online Auction for Vulnerabilities Mulls Shutdown. *DarkReading*.

Hoglund, Greg, and Gary McGraw. 2004. *Exploiting Software: How to Break Code*. Boston: Addison-Wesley.

Howard, John. D. 1997. An Analysis Of Security Incidents On The Internet 1989 - 1995. PhD Dissertation, Carnegie Mellon University, Pitssburgh, Pennsylvania.

IBM. 2007. IBM Internet Security Systems X-Force 2006 Trend Statistics. Atlanta, GA: IBM Internet Security Systems.

———. 2008. IBM Internet Security Systems X-Force 2008 Mid-Year Trend Statistics. Atlanta, GA: IBM Internet Security Systems.

———. 2009. IBM Internet Security Systems X-Force 2008 Trend and Risk Report. Atlanta, GA: IBM Internet Security Systems.

IntelliSIGHT. 2009. 2008 Year- in- Review and Look Forward http://www.isightpartners.com/webdocs/isightpartners_intellisight_2008ye_20090108.pdf.

Kannan, Karthik, and Rahul Telang. 2005. Market for Software Vulnerabilities? Think Again. *Management Science* 51 (5):726-740.

Landwehr, Carl. E, Alan. R. Bull, John. P. Mc. Dermott, and William. S. Choi. 1994. A Taxonomy of Computer Program Security Flaws, with Examples. *ACM Computing Surveys* 26 (3).

Lemon, Sumner. 2008. WabiSabiLabi may Close 0Day Auction Site. *Network World*, October 30.

Leung, Linda. 2005. Color-coding hackers: Learn the Distinctions Between White-, Black- and Gray-hatted Hackers. *Network World*, June 20.

Lipson, Howard F. 2002. Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. Pittsburgh: CERT Coordination Center, Software Engineering Institute, Carnegie Mellon Unversity.

Mass, Nathaniel J. 1980. Stock and Flow Variables and the Dynamics of Supply and Demand. In *Elements of the System Dynamics Method*, edited by J. Randers. Cambridge, Massachusetts: The MIT Press.

Meadows, Dennis L. 1970. *Dynamics of Commodity Production Cycles*. Cambridge, Massachusetts: Wright Allen Press.

Michaely, Michael. 1954. A Geometrical Analysis of Black-Market Behavior. *The American Economic Review* 44 (4):627-637.

Miller, Charles. 2007. The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales. Paper read at Workshop on Economics of Information Security, at Pittsburgh, USA.

Minasi, Mark. 2000. *The Software Conspiracy*. New York: Mc Graw-Hill.

Moore, Tyler, and Richard Clayton. 2008. The Impact of Incentives on Notice and Take Down. In *Workshop on the Economics of Information Security, June 25-28, 2008*. Hanover, New Hampshire.

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

NIST. 2006. Computer Security Incident Handling, edited by K. Scarfone, T. Grance and K. Masone: U.S. Department of Commerce.

Nordin, J. A., and Wayne R Moore. 1947. Bronfenbrenner on the Black Market. *The American Economic Review* 37 (5):933-934.

Organization for Internet Safety. 2004. Guidelines for Security Vulnerability Reporting and Response. http://www.oisafety.org/guidelines/.

Ozment, Andy. 2004. Bug Auctions: Vulnerability Markets Reconsidered. Paper read at Workshop of Economics and Information Security (WEIS), at Mineapolis, MN.

———. 2005. The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting. Paper read at The Workshop on Economics and Information Security (WEIS), at Cambridge, MA, USA.

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

Parker, Don. 2005. The Different Shades of Hackers. *WindowSecurity*, http://www.windowsecurity.com/articles/Different-Shades-Hackers.html.

Penenberg, Adam. 2008. The Black Market Code Industry. *Fast Company*, http://www.fastcompany.com/magazine/127/nexttech-fear-of-a-black-hat.html.

Perloff, Jeffrey. M. 2007. *Microeconomics*. Fourth Edition ed. Boston: Pearson, Addison Wesley.

Radianti, Jaziar, and Jose J. Gonzalez. 2007a. A Preliminary Model of The Vulnerability Black Market. Paper read at 25th International System Dynamics Conference at Boston, USA.

———. 2007b. Understanding Hidden Information Security Threats: The Vulnerability Black Market. Paper read at 40th Annual Hawaii International Conference on System Sciences at Big Island, Hawaii.

———. 2009. Dynamic Modeling of the Cyber Security Threat Problem: The Black Market for Vulnerabilities. In *Cyber-Security and Global Information Assurance: Threat Analysis And Response Solutions*, edited by K. J. Knapp. Hershey, PA: Information Science Reference.

Radianti, Jaziar, Eliot Rich, and Jose J. Gonzalez. 2007. Using Mixed Data Collection to Uncover Vulnerability Black Markets. Paper read at Workshop on Information Security and Privacy (WISP), at Quebec, Canada.

———. 2009. Vulnerability Black Markets: Empirical Evidence and Scenario Simulation. Paper read at 42nd Annual Hawaii International Conference on System Sciences at Big Island, Hawaii.

Radianti, Jaziar, and Nils Ulltveit-Moe. 2008. Classification of Malicious Tools in Underground Markets for Vulnerabilities. Paper read at Norsk informasjonssikkerhetskonferanse (NISK), at Kristiansand, Norway.

Randers, Jørgen. 1980. Guidelines for Model Conceptualization In *Elements of the System Dynamics Method*, edited by J. Randers. Cambridge, Massachusetts: The MIT Press.

Rescorla, E. 2005. Is finding security holes a good idea? . *IEEE Security and Privacy* 3 (1):14-19.

Rich, Eliot, Ignacio J. Martinez Moyano, Stephen Conrad, Dawn M Cappelli, and Andrew. P Moore. 2005. Simulating Insider Cyber-Threat Risks: A Model-Based Case and a Case-Based Model. Paper read at Proceedings of the 23rd International Conference of System Dynamics Society, at Boston.

Richardson, George P., and Alexander. L. Pugh. 1981. *Introduction to System Dynamics Modeling*: Productivity Press, Portland, Oregon.

Richardson, Robert. 2008. Computer Crime and Security Survey. http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf.

Rush, Howard, Chris Smith, Erika Kraemer-Mbula, and Puay Tang. 2009. Cybercrime and Illegal Innovation. In *NIESTA*. Brighton, UK: University of Brighton.

Schechter, Stuart 2002. How to Buy Better Testing: Using Competition to Get The Most Security and Robustness for Your Dollar. Paper read at Infrastructures Security Conference, October, at Bristol, UK.

Schneier, Bruce. 2000. *Publicizing Vulnerabilities* [cited 10 April 2007]. Available from http://www.schneier.com/crypto-gram-0002.html.

———. 2007. *Schneier: Full Disclosure of Security Vulnerabilities a 'Damned Good Idea'* [cited June 19 2007]. Available from http://www.schneier.com/essay-146.html.

Seacord, Robert C., and Allen D. Householder. 2005. A Structured Approach to Classifying Security Vulnerabilities. (December 22), http://www.sei.cmu.edu/pub/documents/05.reports/pdf/05tn003.pdf.

Solomon, Michael G., and Mike Chapple. 2005. *Information Security Illuminated*. Boston: Jones and Bartlett Publishers.

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

Sutton, Michael, and Frank Nagle. 2006. Emerging Economic Models for Vulnerability Research. Paper read at Fifth Workshop on the Economics of Information Security (WEIS), 26-28 June at Robinson College, University of Cambridge, England.

Symantec. 2008a. Symantec Global Internet Threat Report: Trend for July - Dec 07. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf.

———. 2008b. Symantec Report on Underground Economy. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf.

Tassey, Gregory. 2002. The Economic Impacts of Inadequate Infrastructure for Software Testing. http://www.rti.org/pubs/software_testing.pdf.

Telang, Rahul, and Sunil Wattal. 2007. An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price. *IEEE Transactions on Software engineering* 33 (8):544-557.

Wiik, Johannes, Jose J. Gonzalez, Howard F. Lipson, and Timothy J. Shimeall. 2004. Dynamics of Vulnerability-- Modeling the Life Cycle of Software Vulnerabilities. Paper read at Proceedings of 22 nd International System Dynamics Conference, July 25-29, 2004, at Oxford, UK.

Zhuge, Jianwei, Thorsten Holz, Chengyu Song, Jinpeng Guo, Xinhui Han, and Wei Zou. 2007. *Studying Malicious Websites and the Underground Economy on the Chinese Website* [cited February 25 2008]. Available from http://honeyblog.org/archives/2007/12/summary.html.

Zorz, Mirko. 2003. Interview with Sunil James, Manager of iDEFENSE's Vulnerability Contributor Program. http://www.net-security.org/article.php?id=438&p=3.

Appendix

Abbreviation

BH(s)	:	Black Hat Hacker(s)
BM(s)	:	Black Market(s)
CERTs	:	Computer Emergency Response Teams
CC(s)	:	Credit Card(s)
CSI	:	Computer Security Institute
CVE	:	Common Vulnerabilities and Exposures
CVV2	:	Card Verification Value (also called CV2; CVV; or CVC—Card Verification Code, V-Code—Verification Code and CSC—Card Security Code)
DACP	:	Digital Armaments Contribution Project
DoS	:	Denial of Service Attack
EAP	:	Exploits Acquisition Program
ISS	:	Internet Security Systems
IRC	:	Internet Relay Chat
LM(s)	:	Legal Market(s)
NIST	:	National Institute of Standards of and Technology
NVD	:	National Vulnerability Database
OIS	:	Organization for Internet Safety
OSVDB	:	Open Sources Vulnerability Database
SD	:	System Dynamics
VBM(s)	:	Vulnerability Black Market(s)
VCP	:	Vulnerability Contributor Program
Vuln(s)	:	Vulnerability(ies)
VM(s)	:	Vulnerability Market(s)
WH	:	White Hat Hackers
WSL	:	WabiSabiLabi
ZDI	:	Zero Day Initiative

Glossary

Botnet	:	is a large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack. The computer is compromised via a Trojan that often works by opening an Internet Relay Chat (IRC) channel that waits for commands from the person in control of the botnet. Botnet is one of commodities traded in BMs.
Black Market(s)	:	an arena or any arrangement for conducting illegal trading which takes place hidden from public eyes. The trading covers all motives such as to avoid government regulations, to trade prohibited commodities, or to trade commodities that may be utilized for malicious or criminal purpose. In this paper we used in more specific meaning, i.e. black market for vulnerabilities. *See* Vulnerability Black Market(s).
Black Hat Hacker(s)	:	a person who is able to exploit a system or gain unauthorized access through skill and tactics with malicious motives.
Exploit(s)	:	a piece of codes or script that is developed to abused the vulnerabilities in the software to attack the computer network.
Grey Hat Hacker(s)	:	a hacker who has ambiguous ethics and borderline legality
Hacker(s)	:	a person who breaks into computers
Known exploit(s)	:	*see*: public exploit(s)
Malicious mobile agents	:	malicious programs that can be moved, or can move themselves, from one host to another across a network
Malicious Code	:	a general category of programs such as worms and viruses—

		programs that exploit weaknesses in computer software, replicating themselves and/or attaching themselves to other programs. *See* also Virus(es) and Worm(s).
Malware	:	any computer program that harms the computer running it. Typically, malware is installed without the user's knowledge or consent. Different types of malware include spyware, Trojan horses, rootkits, keyloggers, viruses and worms.
Obfuscator(s)	:	a source code in a computer programming language that has been made difficult to understand. A programmer may deliberately obfuscate code to conceal its purpose.
Patch	:	a quick-repair code for fixing software errors, bugs or vulnerabilities (sometimes called a "fix")
Patched exploit(s)	:	is an outdated exploit because the affected vulnerability is patched. In this study, this term is also used to refer to an exploit that is created from patched vulnerabilities
Patched vulnerabilities	:	vulnerabilities that are published and patched, either by vendor or a third party.
Public exploit(s)	:	a proof-of-concept, demonstrative code, partially or fully functional malicious agent such as malware that is publicly available
Published vulnerabilities	:	vulnerabilities that are published but not yet yet patched.
Reported unpatched vulnerabilities	:	*See*: Published vulnerabilities
Secret vulnerabilities	:	discovered vulnerabilities that are not published.
Unknown vulnerabilities	:	latent vulnerabilities that have not been discovered.
Underground market(s)	:	*See* Black Market(s) and Vulnerability Black Market(s).
Zero-day exploit(s)	:	an exploit that is created on the same day or sometimes before the software vulnerability becomes generally known publicly
0-Day exploit(s)	:	*See*: Zero-day exploit(s)
Virus(es)	:	programs that require some action on the part of the user, such as opening an email attachment, before they spread.
Vulnerability(ies)	:	bugs and flaws (caused by programming errors) that give rise to exploit techniques or particular attack patterns
Vulnerability Black Market(s)	:	an arena or any arrangement for illegal selling and buying activities to trade vulnerability exploits and malware or any products taking malicious advantage of the weaknesses in software and computer networks.
White Hat Hacker(s)	:	is a hacker who attempts to break into systems or networks in order to help the owners of the system by making them aware of security flaws, or to perform some other altruistic activity.
Window of Vulnerability	:	the time interval between when a vulnerability announce and patches are released by software vendor.
Window of Exposure	:	the interval between when a virus begins spreading and signature updates are issued by anti-virus vendors.
Worm(s)	:	programs that spread with no human intervention after they are started. *See* also Malicious Code.