

# Toward a Dynamic Modeling of the Vulnerability Black Market

Jaziar Radianti (jaziar.radianti@hia.no)  
Jose. J. Gonzalez (jose.j.gonzalez@hia.no)

Research Cell “Security and Quality in Organizations”,  
Faculty of Engineering and Science, Agder University College, Serviceboks 509  
NO-4898 Grimstad, Norway

## Abstract

*The “black market” for software vulnerabilities makes it in principle possible for criminals and terrorists to launch exploits toward organizations before system administrators have had a chance to apply a corrective patch. To counteract this threat, software vendors and security companies try to establish a legitimate market for software vulnerabilities: They offer rewards for software bugs reported. A system dynamics model is developed to explain the basic traits of this phenomenon. Using model simulations the authors discuss to what extent the attempt to legalize the vulnerability market may help to reduce the vulnerability information circulating in the black market.*

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

## 1. Background: Critical Infrastructure and Securing the Network

The recent discovery that there is a “black market” or “underground market” for software vulnerabilities adds a new and worrying dimension to the protection of key economic sectors and critical infrastructure. These sectors depend crucially on information security for their performance; for some sectors, good information security is tantamount to satisfactory performance with regards to health, safety and environment. Particularly, in the oil and gas industry, the increasing use of remote operations using computer networks (eOperations, now increasingly called Integrated Operations) implies that information security failures can have severe impact on the Health, Safety and Environment (HSE) aspects. This is becoming a new challenge for security management since the growth of the black market could result in more zero day attacks.

The authors’ interest in the vulnerability problem developed from our work with client oil companies that are transitioning from traditional operations on offshore fields to the new mode of

Integrated Operations.<sup>1</sup> Hence, for specificity, the authors use the case of Integrated Operations to highlight some relevant aspects of the vulnerability problem. This said, the authors have to safeguard the interest of our clients, implying that we do not disclose any kind of sensitive information.

The threats to the security of Integrated Operations are basically the same as for other critical infrastructure. Some information security threats as identified by Whitman [1] are relevant for the case of Integrated Operations: Act of human error or failure (accidents, employee mistakes), deliberate acts of espionage or trespass (unauthorized access/data collection), deliberate acts of sabotage or vandalism (destruction of systems or information), deliberate acts of theft (illegal confiscation of equipment or information), deliberate software attacks (viruses, worms, macros, denial of service), quality of service deviations from service providers, technical hardware failures or errors (equipment failure), technical software failures or errors (bugs, code problems, unknown loopholes), technological obsolescence (antiquated or outdated technologies).

As a consequence of the transition to Integrated Operations, the onshore IT network will be merged with the offshore network despite firewall protection. As a result, the company becomes more vulnerable to threats both from hacker attacks and malicious code attacks. The authors concentrate on the software vulnerability problems for this case because previous security incidents in the client company show that malicious code can reach the platform offshore, though it didn't yet compromise the critical network. Whitman's study [2] ranks "deliberate software attacks" and "technical software failures or errors" as the first and second highest of the threats to information security. Whitman claims are similar to those of the CSI/FBI study that virus attacks is the top of information security threat.<sup>2</sup>

The risk of cyber attack to the business include failure of control systems, loss of integrity or control of systems, loss of process monitoring and visibility of plant. This may lead to injuries or loss of life, loss of production, environmental damage, damage to reputation, loss of licence to operate, etc. An overview of the implication of known security failures upon HSE aspects has been presented in a recent paper by Johnsen et al. [2].

Broadly speaking, exploits of software vulnerabilities today have the following characteristics: automated attacks leveraging known and unknown vulnerabilities, collaboration of social engineering and automated attacks, multiple attack vectors and active payloads. There are indications for a growing number of vulnerabilities in software and operating systems that are only known to so-called "black-hat hackers" and for which there is no patch available yet. Black-hat hackers seek to discover software vulnerabilities for malicious purposes. They often share their information with like-minded individuals. Furthermore, there are indications of a growing black-market for vulnerabilities<sup>3</sup> (hackers selling secret information about software vulnerabilities in COTS (Commercial-off-the-shelf) software to criminals or even terrorists groups).

To minimize risks that may jeopardize the future of Integrated Operations, multiple defense solutions have been proposed: From security monitoring, password protection and secure segregation to security culture, such as improved communication about security incidents, and user awareness and education. Since software vulnerabilities are constantly being discovered, administrators have to deploy new patches that remove the exploitable bug in the software. The situation is complex, though, due to trade-offs of risk patching vs. risk of not patching, as well as planned vs. unplanned downtime (Figure 1).

---

<sup>1</sup> For a short overview of Integrated Operations, see the Appendix.

<sup>2</sup> See, 2006 CSI/FBI Computer Crime and Security Survey, [http://i.cmpnet.com/gocsi/db\\_area/pdfs/fbi/FBI2006.pdf](http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf), quoted September 20, 2006.

<sup>3</sup> See , <http://www.pcpro.co.uk/news/84523/black-market-thrives-on-vulnerability-trading.html> quoted June 13, 2006

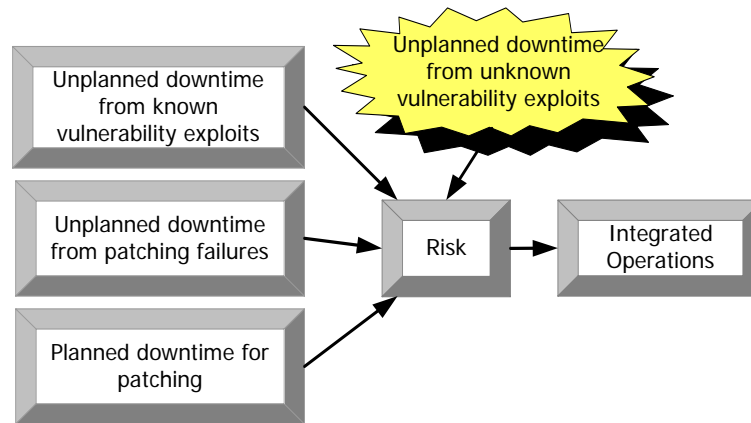


Figure 1. Risk, patching and downtime: Exploits can occur from known and unknown vulnerabilities; exploits can cause unplanned downtime; planned downtime is necessary for testing and application of patches.

The number of unknown attacks<sup>4</sup> exploiting software vulnerabilities is still growing. The potential security impact of unknown attacks is increasing too [3]. However, evidence is mostly anecdotal and circumstantial; good data is scarce. This fact restrains insights, making it difficult to learn from the root causes. Nevertheless, the Honeynet project has provided interesting information about the occurrence of unknown attacks and the increase of the black-hat hacker's activities.<sup>5</sup> Further results from the Honeynet project [4, 5] describe security tools, tactics and motives of the black-hat community. Black hat hackers aggressively scan the Internet for hosts vulnerable to a single "unknown vulnerability," exploiting as many systems as possible. The issue of unknown attacks and the circulation of vulnerabilities in a 'black market' have been getting increasing attention recently. Some security companies also start to identify the presence of the black market and the organized computer crimes as a part of the today's threat.<sup>6</sup> Moreover, Schneier states that organized crime is likely to be better funded, better skilled and better organized than lone criminals, than hackers are.<sup>7</sup>

To discuss this issue, we cannot consider the unknown vulnerability exploits as a security concern only, we have to take the economic dimension of the security problems into consideration too. This paper discusses vulnerability exploits and the importance of patching vulnerabilities in the context described in Figure 1. In the next section, we discuss the black market vulnerability problem and the shifting trend towards a "legal" vulnerability market and the implications of the alteration. A simple system dynamics model about the likely growth of the vulnerability black market is developed. Finally, we return to the security policy in Integrated Operations and we discuss related topics for the general software *end-user*.

A note on terminology: We use "hacker" in the sense of a "black-hat hacker" – a person who is able to exploit a system or gain unauthorized access through skill and tactics, and not to refer white-hat hacker. It is necessary to clarify the terminology because there are several terms in the literature to identify the people searching the vulnerabilities such as: "bug bounty hunters" [6],

<sup>4</sup> Unknown attack is defined as an attack against a vulnerability nobody has heard of.

<sup>5</sup> See for example <http://www.honeynet.org/papers/stats/> about attack by black hat community, quoted 13 June 2006

<sup>6</sup> See for example *The Security Guide 2006* from AppSense.

<sup>7</sup> <http://www.ffpress.net/Kunden/APP/Downloads/APP85333/APP85333.pdf>, quoted September 20, 2006

<sup>7</sup> See interview with Bruce Schneier, <http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/schneier.html>, quoted September 20, 2006.

“flaw researchers”, “vulnerability researchers” [7], “testers” [8, 9]. In addition, vulnerabilities are discovered by people with a spectrum of intentions from *bad* (“black-hat”) to *good* (“white hat”).

By “malicious agents” we refer to other actors having malicious motives to compromise security, but without skill for doing so; they could be criminals, terrorist groups or just “script kiddies”.

## 2. Vulnerability Black Market Problems and Vulnerability Market Solution

All discussion about software vulnerability problem from an economic perspective consider software as a ‘market for lemons’, see Anderson [10], Schechter [8], Ozment [9] and Böhme [11, 12]. This term is introduced by Akerlof [13]. The author describes how the interaction between quality heterogeneity and *asymmetry of information* can lead to the disappearance of a market where guarantees are indefinite. When quality is unascertainable beforehand by the buyer (due to the asymmetry of information) incentives exist for the seller to pass off a low-quality good as a higher-quality one. The buyer, however, takes this incentive into consideration, and assesses the quality of the good to be uncertain. Only the average quality of the good will be considered, which in turn will have the side effect that goods that are above average in terms of quality will be driven out of the market.

In the software market case, the buyer is indeed unable to distinguish between secure and insecure products. Hence, the vendor has little incentive to develop a better security technology. As Schechter says [8, p.1]: “A market for lemons is one in which the consumer cannot determine products of quality from defective goods.” According to Schneier it happens because the marketplace doesn’t reward security. A big software company could spend an extra year developing the new version of software application and involve more people in testing security problems in the software, but then the software would be released one year later to the market.<sup>8</sup> A tendency to use the principle of ‘penetrate and patch’ for software producers may create many security problems among software users.

In every market, there are sellers and buyers. They are the fundament of trade, along with the actual exchange of goods and services and the associated transaction. If the number of buyers increases, the number of sellers tends to increase as well. In particular cases, e.g. when there are incentives for criminal activities, a black or underground market tends to appear. We believe that the vulnerability black market, too, is governed by the laws of supply and demand. As long as there is someone willing to pay, there will be someone willing to sell.

It has been mentioned that vulnerabilities might be discovered by people with an interest in exploiting it. Instead of notifying the vendor, they take themselves advantage of the vulnerability and potentially inform some of their associates. Information about the vulnerability circulates in the hacker community and the vulnerability may be exploited (by a limited numbers of hackers) before it becomes known publicly. Neither vendors, nor users are conscious of this threat.

It has been suggested that there is a massive underground trade in software vulnerabilities, particularly during the period of private disclosure (see footnote 3). Organized crime pays high prices for information that helps to break into corporate databases for identity theft and other lucrative criminal activities.

Hackers seek out vulnerabilities mainly to improve their opportunity for financial gain through successful exploitation. But recently this phenomenon has been shifting character.

---

<sup>8</sup> See Kim Zetter, *Three Minutes With Security Expert Bruce Schneier*, 2001. Available from <http://www.pcworld.com/article/id,63806-page,1/article.html>, quoted August, 30, 2006.

Hackers find unknown vulnerabilities and sell them to the highest bidder. An example of how hackers advertise their findings can be found in the Web Security Trend Report by Finjan [14]. Hackers start considering the private disclosure of a vulnerability as a business opportunity. Itzhak [15] calls it the “malicious code food-chain”.

Hackers use the Internet as the main channel for sharing information about exploiting software vulnerabilities and exposures. Since the number of Internet users is growing and intruder tools are becoming more sophisticated and easier to use, more people can become “successful intruders”. In addition, malicious code developed lately is easy to launch remotely. It might be a source of attractiveness to buy “secret vulnerabilities”. Schechter [16] states: “Staging an attack without being identified is preferable to staging an attack and avoiding prosecution. Network attackers regularly hide their identities by routing their communicating through sequence of distant systems. The longer the trail, the harder it is to trace its source...” Data also show that vulnerabilities exploited remotely nowadays show an increasing trend (Figure 2).

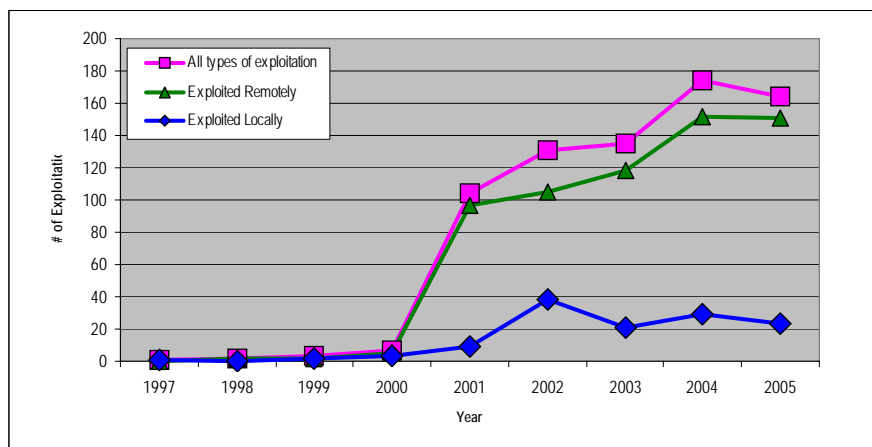


Figure 2 Trend of Vulnerability Exploitation

Sources: National Vulnerability Database Statistics (<http://nvd.nist.gov/statistics.cfm>)<sup>9</sup>

It is still difficult to determine if the raising trend of vulnerability exploitations performed remotely has a positive correlation with the emergence of the black market vulnerabilities. However, research by the HoneyNet Project shows the increase of black-hat activities. It also states that security in organization is still in question due to a challenge of new attacks threats or security software is not aware of.

Attempts to protect the software user from software vulnerabilities in pre- and post-release phases through the vulnerability market mechanism as a solution had been discussed lately in several studies. We omit the discussion about the vulnerability life cycle and exploitation as discussed by some authors. Sutton and Nagle [7] classify the current vulnerability market discussion as government market, open market, underground market, auction market and vendor market. A different concept of the vulnerability market is introduced by Böhme [11, 12]. His main purpose in describing a different concept of the vulnerability markets is to discuss its advantages and to identify the best market type where security-related information can be traded and to find which type serves best to counter security market failures.

<sup>9</sup> It is searched base on following criteria: occurred between January 1998-December 2005; launched remotely and locally, has high severity level of vulnerability and using US-CERT Vulnerability Note

Originally Böhme proposed five kinds of vulnerability markets [11] but then Böhme revisited the literature and he proposed four market alternatives [12]: Bug challenges, vulnerability brokers, exploit derivatives and cyber-insurance. To begin with, Böhme differentiated between Bug Challenges and Bug Auction, but now he merges them into one category (“Bug Challenges”). Basically, all proposals aim at motivating software developers to take security more seriously.

Schechter [8] for example, proposes that vendors/security firms create a vulnerability market in order to ascertain the cost to break of their system. Schechter’s main proposal is to offer an economic approach where a producer would offer rewards at the market price to the first testers (persons or organizations who identify vulnerabilities in return for payment) who inform the producers of new vulnerability in their product. The market price is governed by the competition among those testers. A good market has a rule about *the cost of finding vulnerabilities, the speed of finding and the order in which vulnerabilities are found* to buy testing. But then he argues that the good market should have the following rules: *access, pricing, selling and information*. Andy Ozment [9] first formulated the vulnerability market as a bug auction theory. Ozment argues that the ‘bug auction’ theory based on the “Dutch auction” template has a key advantage: a reward is always offered, ensuring what vulnerabilities are reported immediately if they are being traded on the black market. He compares it to an “English auction” type that requires a waiting period and the delays could cause a tester to first sell a vulnerability on the black market.

The authors concur with Schechter that the security and robustness of software systems traditionally has suffered because testers have not been properly rewarded. However, the authors consider this phenomenon a realistic explanation of why the vulnerability black market emerges and proliferates. The basis to observe the vulnerability market problem from this viewpoint is the emergence of a recent phenomenon that the computer security enterprises are creating legitimate markets for vulnerabilities. Security companies argue that this legal market approach will give them critical information so they can enhance their protection service to the client.<sup>10</sup> To our understanding the legal vulnerability market is created to alter the relationship depicted in Figure 3. This is no longer only a theoretical discussion. For those reasons we raise a question: how does the black market vulnerability emerge and grow?

An effort to explain how the underground vulnerability market mechanism (“the black market”) works is found in a paper from Sutton and Nagle [7]. They introduce the *contracted model* and the *purchase model*. In the former model the malicious actor hires a hacker to find a vulnerability in a specific target. However, they underline that there is little public information on the contracted model. The purchase model is done in reverse from the contracted model. In that model the hacker

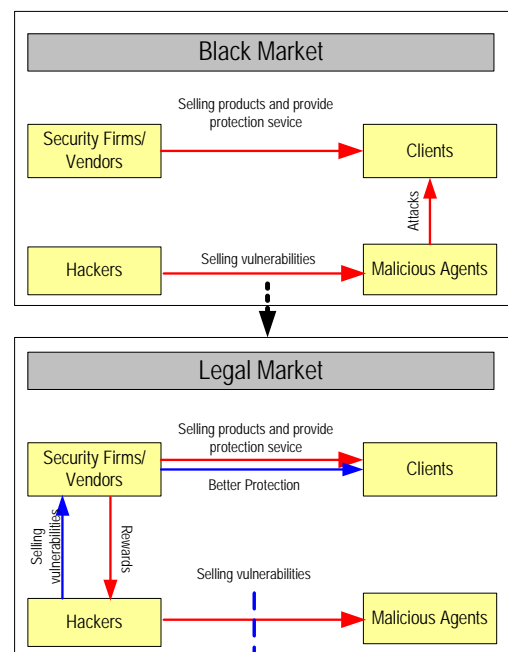


Figure 3  
From Black Market to Legal Market

<sup>10</sup> For instance, one security firm launches a market called “Zero Day Initiatives”. See [http://www.businessweek.com/magazine/content/05\\_34/b3948022\\_mz011.htm](http://www.businessweek.com/magazine/content/05_34/b3948022_mz011.htm); <http://www.informationweek.com/showArticle.jhtml?articleID=180204079>, see also debate on this <http://www.networkworld.com/columnists/2005/091205faceoffno.html>, quoted on 13 June 2006.

finds a vulnerability, creates an exploit and sells it to the malicious actors. Sutton and Nagel [7] emphasize that all parties have to broker the deal, involving some potentially risky contracts, while making sure that they are not caught by law enforcement. The market mechanism can be described in following diagram:

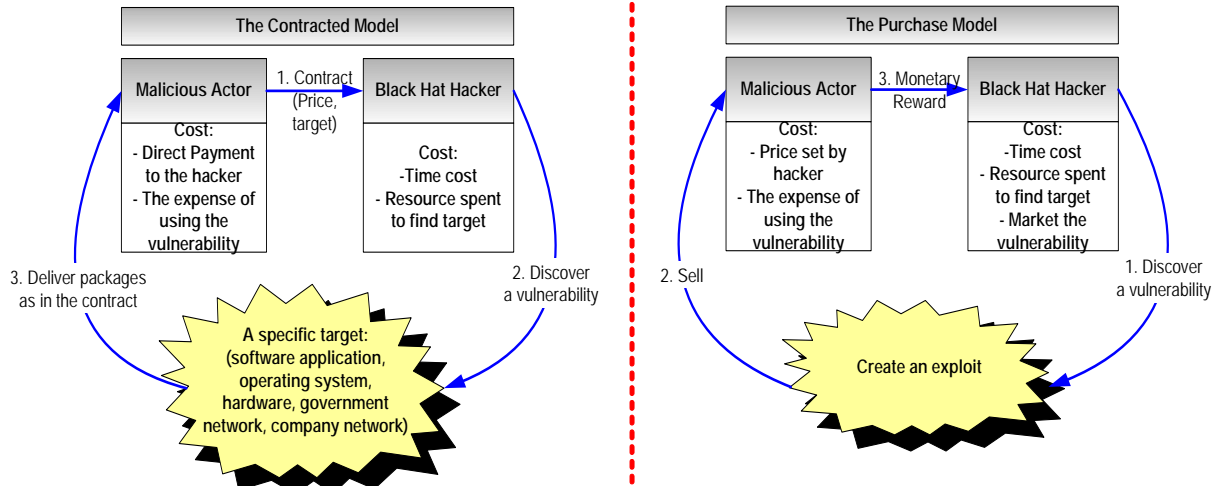


Figure 4  
 The contracted model and the purchase model in the Black Market

In this paper, the market mechanism is looked upon as a means to shift the vulnerability black market to a ‘legal’ market, and to detect potential problems that may arise as unintended consequences of the change in the vulnerability market pattern. The system dynamics approach is employed to build a preliminary model that can capture the basic structure of the problem. The model developed for this paper is an idealized version of the purchase model.

### 3. Black Market Vulnerability Model

#### System Dynamics

System dynamics is a method to enhance learning in complex systems [17]. Richardson and Pugh [18] state: ‘The system dynamics approach to complex problems focuses on feedback processes. System Dynamics takes the philosophical position that feedback structures are responsible for the changes we experience over time...dynamic behavior is a consequence of system structure.’ System dynamics is demonstrably efficient for knowledge capture – especially of huge amounts of fragmented (formal and tacit) data and knowledge. It has an ability to create causal maps, to analyze those causal maps, to create ‘dynamic stories’ that visualize the behavior of complex security systems, to create team/ organizational learning and to generate policies to manage complex systems.

Also, compared with other modeling methods aimed at making predictions, the system dynamics objectives are to increase understanding of some observed phenomenon, consequences of different options available at a decision point and not so much to generate predictions [19].

System dynamics is becoming a popular method to model information system security owing to its ability to «..., provide[s] a foundation for developing methods and tools that help engineers understand, characterize, and communicate the impact of a malicious threat environment on

organizational and system operations and their respective missions. Large-scale, inter-networked information systems are subject to volatility, nonlinearity, uncertainty, and time delays that add to their dynamic complexity and make assuring their security or survivability so difficult.» [20, p. 38ff]

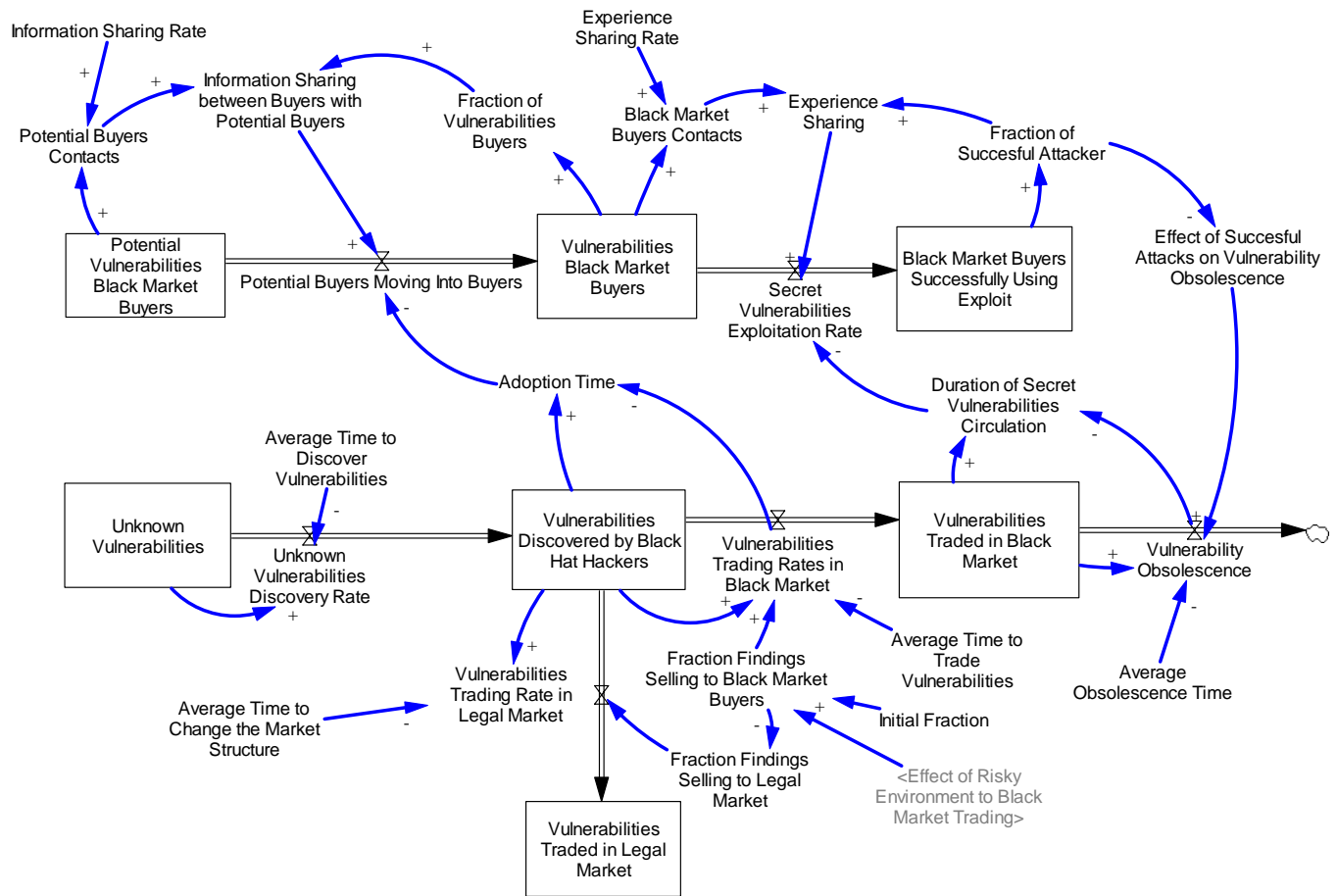


Figure 5. The black market vulnerability growth model

### Model Description

The Vulnerability Black Market does work as a market since there is a supply side, namely hackers, and a demand side, viz. malicious agents or criminals. Our simple model explains the growth of the vulnerability black market: On the demand side, there are a group of people who are willing to pay for secret knowledge about new vulnerabilities; on the supply side, hackers develop scripts of malicious code after they discover vulnerabilities. Hackers are finding new vulnerabilities and developing exploits, and then selling the whole package to the highest bidder—who most likely is criminal group. It is assumed that hackers do not want to execute the exploits themselves out of concern for their own safety.<sup>11</sup>

<sup>11</sup> Because hackers more and more frequently are being prosecuted, as the appropriate legislation is being implemented. See for example the case of Mitnick <http://archives.cnn.com/2000/TECH/computing/01/21/mitnick.release.01/index.html>; hackers face life imprisonment under 'Anti-Terrorism' Act, see <http://www.securityfocus.com/news/257>.

Figure 5 uses a graphical notation based on three different types of elements: *stocks*, *flows*, and *information*. This graphical notation also is used as a basis for developing a quantitative model which can be used to study the characteristics of the process. The stock and flow diagram shows relationships among variables which have the potential to change over time. For example in the model, the variables *Unknown Vulnerabilities*, *Vulnerabilities Discovered by Black Hat Hackers* and *Vulnerabilities Traded in Black Market* are shown inside rectangles. This type of variable is called a *stock*, *level* or *accumulation*. The variable *Unknown vulnerabilities Discovery Rate* is shown as a “valve” symbol. This type of variable is called a flow or rate.

A double line arrow pointing from *Unknown Vulnerabilities* toward *Vulnerabilities Discovered by Black Hat Hackers* looks like a pipe and the ‘valve’ controlling the flow through the pipe. This says that there is a flow from *Unknown Vulnerabilities* to *Vulnerabilities Discovered* with a rate controlled by the *Unknown Vulnerabilities Discovery Rate* valve. And the idea behind the difference between a stock and a flow: A stock is an accumulation of something and a flow is the movement or flow of the “something” from one stock to another. The last element in the Figure 5 is the information link shown by the curve arrow. This arrow means that in some way information about the value of the variable influences the other variables.

The main structure of the model (Fig. 5) consists of two connected aging chains (“co-flows”). The aging chain in the bottom part depicts three stages of unknown vulnerabilities: before they are discovered until they are traded in the black market. The aging chain in the upper part shows three stages of black market buyers: from potential vulnerability black market buyers until they become successful intruders. In this simple model, the discovery rate of unknown vulnerabilities depends on the speed of disclosure. In this model the speed of disclosure is represented by *Average Time to Discover Vulnerability*. Once the vulnerabilities are discovered, they will be traded in black market; this is described in the model by the causal links connecting the vulnerability aging chain with the buyers co-flow structure. The circulation of such vulnerabilities will shrink after the vulnerabilities become publicly known. The model assumes that the rate of finding the unknown vulnerability by hackers is much faster than by other parties, particularly vendors. This assumption is influenced by Schneier’s opinion: “....There are thousands of people looking for security bugs, so they're bound to stumble upon them. It might take days, weeks, months--there are just so many holes to find. I'm sure the software companies do some testing and find some holes, but they're not doing a lot....”<sup>12</sup> Schneier doesn’t explicitly state that hackers must be faster than vendors in finding vulnerabilities. But owing to market pressure to release software products, security is considered as secondary in the priority of producers. And hackers are likely faster to find the undetected flaws in the software products.

Are criminals or terrorist organizations the only potential buyers of yet unreported vulnerabilities? There are other actors, namely the security companies and vendors of software, and there are recent indications that they offer rewards on reports about yet unknown vulnerabilities. We capture this by the rate *Vulnerability Traded to Legal Market* flowing from the stock *Vulnerability Discovered by Black Hat Hackers* to the stock *Vulnerabilities Traded in Legal Market*.

Assume that there are criminals who are willing to pay a higher price for secret vulnerabilities. In the model they are represented by the stock *Potential Vulnerabilities Black Market Buyers*. It takes some time until potential buyers get information about new vulnerabilities and they form a decision to buy it. When hackers advertise their findings online, we assume it is intended for a group of potential buyers. In order to become a real buyer, a

---

<sup>12</sup> See Kim Zetter, *Three Minutes With Security Expert Bruce Schneier*, 2001. Available from <http://www.pcworld.com/article/id.63806-page.1/article.html>, quoted August, 30, 2006.

potential buyer needs to be convinced that he will get a financial gain by investing his money on an unknown exploit.

One of marketing theories of the consumer behavior may help explaining how potential buyers become real buyers. We cannot compare on-line criminal buyers' behavior in our case with buyers of daily products in the market, but there is a theory that should also be applicable in explaining our case. Every buyer needs recognition of the products, information search, and evaluation before purchase [21]. We assume that buyers as consumers, even criminals need recognition, information search, and evaluation before making a purchase decision.

To recognize a product, a buyer can obtain information from personal, commercial, public or experiential sources. Personal sources (so-called "word of mouth") are sometimes more be trusted than commercial or public sources. Strauss and Frost say, Internet is especially well suited for word-of-mouth communication because of email, newsgroups, chat and personal Web pages [21]. In our case, there should be a mechanism so that potential criminal buyers can obtain information about unknown exploits. Personal contact may be more reasonable as a source of information searching. The uniqueness of the Internet lies in the fact that it is not a system owned by one individual, company, state authority or country. As such there is almost unlimited access to information of all kinds, more and more of which is being used in criminal activity. Criminals are highly attracted to the possibility of unlimited criminal information exchange.<sup>13</sup> Sutton and Nagel specify: "...There are numerous underground websites and IRC chat rooms that are created specifically for putting malicious actors in touch with vulnerability researcher..." [7, p. 10].

"High-involvement purchases" is a term denominating purchases carrying high expenditure or personal risks. One would expect a high degree of involvement with regard to software vulnerabilities because the potential buyer needs complete information and risk assessment. Although we do not explicitly model this process, the rate *Information Sharing between Buyers with Potential Buyers* captures the idea of high-involvement of the buyers.

*Fraction of Vulnerabilities Buyers* is the percentage of the buyer population who may share information with similarly minded people. Information sharing even reinforces the decision process to "purchase" vulnerabilities. Once purchased, the vulnerabilities lead to exploits (*Secret Vulnerabilities Exploitation Rate*) than increase the stock *Black Market Buyers Successfully Using Exploit*.

Now we consider the interaction through experience sharing between *Vulnerabilities Black Market Buyers* and *Black Market Buyers Successfully Using Exploit*. Rogers [22] has successfully applied social learning theory<sup>14</sup> to explain criminal computer behavior. Rogers refers to Hollinger's research showing that individuals are more likely to be involved in illegal computer activity if they have friends who also engage in the activity. In addition, citing Chandler and Taylor study, Rogers summarizes: "...The structure of computer underground itself may be partially responsible for the high rates of differential association and differential reinforcement. Studies have indicated that individuals involved in criminal computer behavior associate with other computer criminals either virtually through chat channel or newsgroup or physically by way of conference and conventions." Regarding moral engagement, Rogers quotes Bandura's research that individuals who use moral disengagement are more able to justify and rationalize their deviant activities, thus continuing their behavior.

---

<sup>13</sup> See <http://library.thinkquest.org/04oct/00460/criminal.html>

<sup>14</sup> Social learning theory is a well-known theory for understanding traditional criminal behavior. Criminal behavior could be learned at the cognitive level through observing other people's actions. Once the behavior is learned it may be reinforced by the consequences it generates. A theory called 'differential association theory' basically says that criminal behavior was learned through a process of interaction with others.

Furthermore, Rogers [22, p. 144-145] quotes Chantler: ...“It has been speculated that criminal computer behavior may in fact be more dependent on differential association than general criminal behavior. The unique technical requirements of criminal computer behavior as opposed to general criminal computer behavior would dictate that individuals wanting to engage in the behavior would have to learn the skill...this skill must be acquired by associating with others who already have the knowledge and skills.”

We adopt the above mentioned theory that criminal behavior is learned through a process of interaction with others as an explanation for why more people become successful intruders. In the model the criminal activity is depicted by a flow from *Vulnerabilities Black Market Buyers* and *Black Market Buyers Successfully Using Exploit* which is affected by *Experience Sharing*.

Why would black-hat hackers prefer selling their findings to criminals? The likely answer is that the reward offered by criminals is higher than the rewards offered by vendors. In other words, black hat hackers will sell their findings to the highest “bidder”.

In our model, hackers are assumed to be rational actors and they will sell their finding to the parties offering the highest price. The authors describe the hacker’s decision process by the parameters *Fraction Findings Selling to Legal Market* and *Fraction Findings Selling to Black Market Buyers*. *Fraction Findings Selling to Black Market Buyers* is modeled as a constant and *Fraction Findings Selling to Legal Market* is defined as  $(1 - \text{Fraction Findings Selling to Black Market Buyers})$ . These parameters describe the fraction of hackers’ findings that will be sold to the black market and the legal market, respectively. The model initially assumes that hackers sell all their findings to the black market since the reward is bigger than for the legal market. That is, at the outset the parameter *Fraction Findings Selling Legal Market* has the value of zero, implying that 100 percent of hacker’s findings are traded to the black market. By changing the value of the parameter one obtains different simulation scenarios with varying degrees of trading to the black market.

By market structure we mean a description of the behavior of buyers and sellers.<sup>15</sup> We expect that the emerging vulnerability market could change the behavior of sellers (*hackers*) to sell their findings on legal market and could contain the black market proliferation. However the legitimate market cannot suddenly alter the legal market, because the change needs time. Sutton and Nagel [7] describe the challenges that may become sources of time delay, such as convincing security researchers to contribute vulnerabilities, gaining acceptance within the industry and developing revenue stream from legitimate market. We describe the temporal extent of this delay by the parameter *Average Time to Change the Market Structure*. The outflow from *Vulnerabilities Discovered by Black Hat Hackers to Vulnerabilities Traded in Legal Market* is affected by *Average Time to Change the Market Structure* and *Fraction Findings Selling to Legal Market*.

Vulnerabilities cease to be traded in the black market mainly because of two factors: 1) vendors find a patch to fix vulnerabilities or 2) post-depreciation phase, when the producer is no longer interested in actively improving the product or its security, usually because a successor product has become available. In this model this is captured by the outflow *Vulnerability Obsolescence*. In addition there is another feedback affecting as well the outflow from *Vulnerability Traded in Black Market*, namely *Effect of Successful Attacks on Vulnerability Obsolescence*. This is to capture: The more people succeed using unknown exploits, the faster the vendor develop patch.

---

<sup>15</sup> We don’t connote ‘market structure’ here in more specific meaning such as a pattern formed by the number, size, and distribution of buyers and sellers in a market (monopoly, duopoly, oligopoly, etc).

**Adding a Riskier Environment into the Model**

Now we add a risk into the model. A hacker identifies vulnerabilities in the software applications, can sell them for \$ 4,000 on the black market or \$ 1,000 on the legal market. Hackers are assumed to be rational actors. Now, there are two considerations for hackers to sell vulnerabilities on the black market: the financial gain and the risk of being caught by the law enforcement. Suppose a hacker consider selling his findings on the black market. For simplicity we concentrate on situations in which there are only two possible outcomes. If a hacker finds a buyer(s) and sells the secret vulnerability, he will earn \$4,000 but he also has a risk of being caught by law enforcement. We assume the cost of going into jail is the same as his earning if he sells to the black market and the cost of finding the vulnerabilities is assumed to be zero. If he sells to the legal market, he earns less income (\$ 1,000). A hacker also has a possibility of failure, say if other people also find a similar bug. Since we assume the cost of finding is zero, he won't earn anything, but he has no risk being caught by legal officers. And the situation is summarized in the following table:

**Table 1**  
**Outcomes of Selling on the Black Market and the Legal Market**

	<i>Outcome 1 (Succeed)</i>		<i>Outcome 2 (Failure)</i>		<i>Expected Value<sup>16</sup></i>
	Probability	Income	Probability	Income	
Sell to Black Market	0.6	\$4,000	0.4	-\$4,000	\$ 800
Sell to Legal Market	0.8	\$1,000	0.2	\$ 0	\$ 800

One such measure of risk is the variance and standard deviation (SD,σ). In our case, SD to sell on the black market is \$ 1,959 and to sell on the legal market is \$ 357.77. If the EV is constant, the smaller the standard deviation or variance, the smaller the risk is. Therefore although the EV is the same on both markets, we can conclude that selling to the black market is riskier than selling to the legal market.

Will a hacker sell his findings on the legal market or the black market? To answer such question, we need to know a hacker's attitude toward bearing risk. In a theory of decision making under uncertainty, whether people choose a risky option over a non-risky one depends on their attitudes toward risk and on the expected payoffs of each option.

Table 1 illustrates that hacker's expected value is equal if he sells the vulnerability on the black market or the legal market. But the standard deviation of his income is bigger on the black market than on the legal market. It means, to sell vulnerability on the black market involves more risk. The hacker will earn more if he can avoid law enforcement or loose more if he is being caught. He'll sell to the black market if he is a "risk lover".

If people made choices to maximize expected value, they would always choose the option with the highest expected value regardless of the risks involved. However, most people care about the risk as well as expected value. Indeed, most people are "risk averse" and will choose a bundle with higher risk only if its expected value is substantially higher than that of a less risky bundle.

We capture the situation into our system dynamic model. We also incorporate perceived risk concept so that the model is able to show whether hacker's attitude will change over time depend on the perceived risk.

<sup>16</sup> EV to sell on the black market is:  $[Pr(succeed) \times Value(succeed)] + [Pr(caught) \times Value(caught)]$   
 EV to sell on the legal market is:  $[Pr(succeed) \times Value(succeed)] + [Pr(competitor) \times Value(competitor)]$

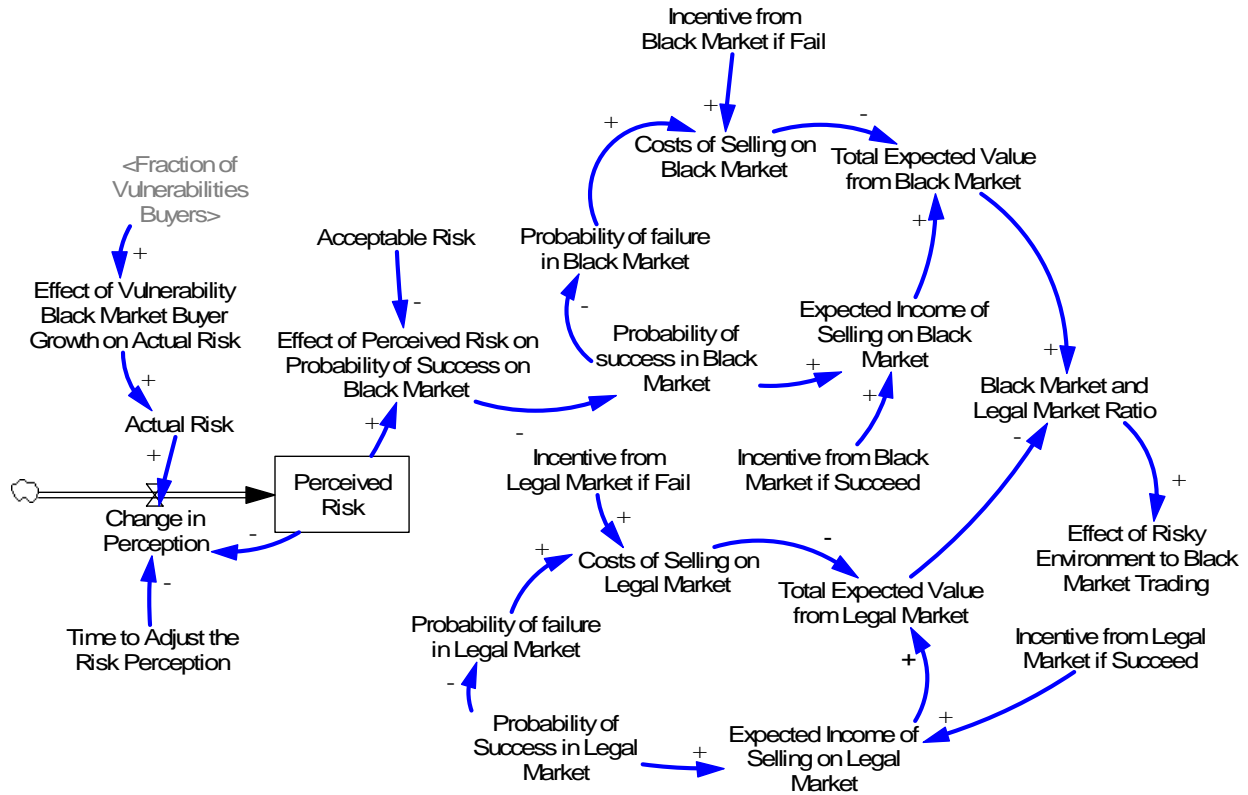


Figure 6  
 The Risk Sub-Model

*Perceived Risk* in the model is depicted as a perception delay of hackers toward risk, and the concept shows of how hacker adjusts his perception with actual risk. People need a time to feel that the environment is riskier than he perceived. The model starts with a low perceived risk. The change in actual risk is affected by the feedback from the vulnerability black market buyer growth (See Figure 5).

A hacker will sell to many buyers unless he is trying to protect his own reputation. But a hacker with a reputation is also a hacker that the police want to arrest. For a seller, increasing the reputation will increase the likelihood that he will be arrested. We capture the above situation through *Effect of Vulnerability Black Market Buyer Growth on Actual Risk*. When the growth is becoming higher, actual risk is becoming higher as well. And a hacker has to adjust his perceived risk in accordance to the actual risk.

*Black Market and Legal Market Ratio* is a calculation of the expected value of selling on the black market or the legal market. If EV on the black market and the legal market are equal, the value will be one. In the model, the hacker prefers selling bugs on the black market if the ratio equal to one. But when EV on the black market < EV on the legal market, rational hackers will sell it on the legal market. This gradual change in the model occurs as the *Perceived Risk* becomes higher. Higher Perceived risk reduces the probability of success for selling vulnerability on the black market. But there is still ‘tolerance’ limit from hackers; we called it *Acceptable Risk*. Higher perceived risk is considered safe as long as it is below the acceptable risk. As the value moves higher than acceptable risk, it means the environment is riskier. Therefore the probability of success to sell vulnerabilities on the black market is becoming smaller. And it

means less expected value from the black market. Once a hacker learns that risk increases and probability of success of selling on black market as well as the expected value shrink, he prefer selling a vulnerability on the legal market. This is portrayed by variable *Effect of Risky Environment to Black Market Trading* (See Figure 5); this variable will affect the flow of *Vulnerabilities Trading Rates in Black Market*.

#### 4. Simulations

We use the simulation software Vensim to develop and simulate the model. We run a simulation with three different scenarios to answer these ‘what-if’ questions:

- What happens if communication and technology available today allow the criminals and hackers to share information and share experience about unknown vulnerabilities and successful attacks?
- What occurs if vendors are able to develop patches faster in order to constrain the criminals’ opportunities to exploit unknown malicious code?
- What happens if vendors establish a legal market as a countermove against the black market?
- What happens if the environment is riskier for selling vulnerabilities on the black market?

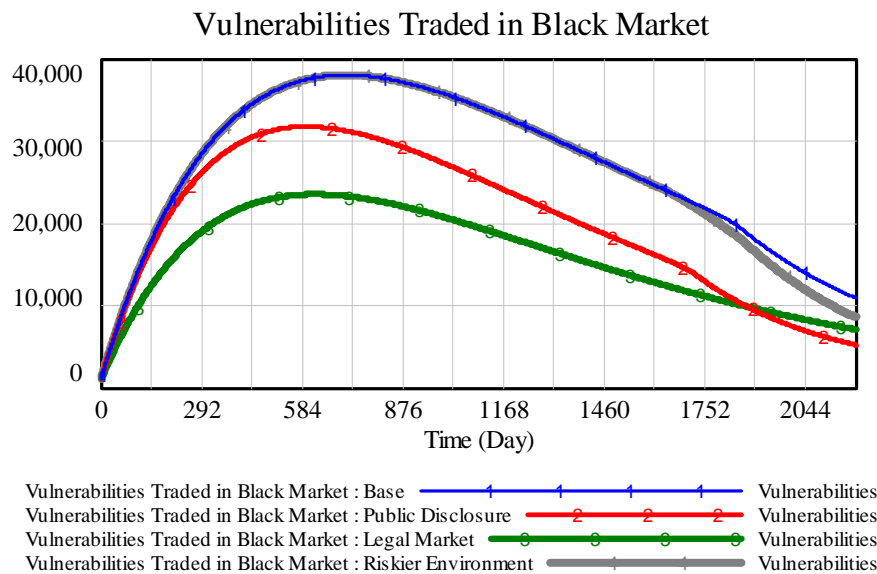


Figure 7 Simulation Results of ‘*Vulnerabilities Traded in Black Market*’

Fig. 7 shows how our model answers these questions. The first plot (thin line, blue) shows the base-run for the model simulation, providing the answer to the first question. The run represents the growth of the black market vulnerability over time (6 yr simulation period). Information and experience sharing between vulnerabilities buyers on how to attack computer networks facilitate the market expansion. The curve rises at the beginning as the malicious agents buy vulnerabilities in the absence of competition from vendors. As the pool of unknown vulnerabilities decreases, trading decreases too. Hence, the growth in *Vulnerabilities Traded in Black Market* flattens out over time and starts declining. However we could observe as well that near the end of the simulation time, it declines faster, since effect of attacks on vulnerability obsolescence start working. If more buyers use an exploit, that vulnerability is more likely to be

discovered. Sellers have incentive to sell to many buyers, thus causing the vulnerability to be discovered by the vendor more rapidly.

The second plot (medium thin line, red) shows the behavior of *Vulnerabilities Traded in Black Market* when the vendor is able to discover the unknown vulnerabilities and to develop a corrective patch faster. The simulation illustrates the growth trend at the beginning, but at a slower pace than the base-run, owing to the vendors' activities. After a peak, which occurs earlier than in the base run, *Vulnerabilities Traded in Black Market* decays faster than in the base run. This is a tentative answer to the second question. However, this scenario might be too idealized: The security companies/ vendors might need some time to realize that their software products are experiencing unknown attacks; and they might even need longer time to develop a corrective.

The third plot (medium thick line, green) represents the effort to transform the vulnerability market by offering rewards to hackers<sup>17</sup> who find security holes in software products. The simulation is carried out by reducing the fraction in the parameter *Fraction Findings Selling to Black Market Buyers*. We assume that 30% of hackers' findings are sold to the legal market. The simulation result shows that this scenario reduces the vulnerability traded in the black market since the simulation initial time. But the trend still grows before it flattens out over time and starts decaying. We explain this behavior because some hackers still sell a certain amount of their findings to the black market. This provides an answer to the third question.

The fourth plot (thick line, grey) shows the simulation when the hacker sells his findings to the legal market and not to the black market. But it occurs later after the risk is becoming higher. Other assumptions for this simulation are the same as the first run, but this time we take a risk into consideration. As long as perceived risk is below the tolerable risk, we can see the behavior is the same as the first simulation. It implies that hackers still sell vulnerabilities on the black market. But near to the end of simulation time, as the environment becomes riskier, the vulnerability traded in the black market starts declining faster than the first plot. There are two effects responsible for this faster declining behavior: effect of risky environment and effect of higher successful attack. The latter causes vendors to develop a patch quicker and shorten the duration of vulnerability circulation. In addition, the fourth scenario works slightly differently from the third scenario on how the reducing process of vulnerability in the black market occurs. The effect of a legal market is driven strongly from the exogenous variable "*Fraction Findings Selling to Black Market*" in scenario three. But in the fourth scenario the reducing process happens because of higher perceived risk of the system.

To summarize, the main notion from the simulations is that the vendors and the security companies have a very significant role in combating or reducing the expansion of the vulnerability black market. *End users* buy, use and patch when necessary, but they can't perform anything to prevent incidents from unknown vulnerability exploits. Therefore, the discussion about the shift of the vulnerability market toward legality becomes relevant for how to contain the vulnerability black market expansion. But attempting to create legal market alone without support from more serious legal action on cyber crime (that may create the riskier environment for the hackers), may affect risk lover hackers to keep selling the bugs on the black market.

## 5. Implications and Future Work

Referring to the case of an oil company that is transitioning to Integrated Operations, the client company is conscious of the importance of patching (in addition to other security measures). The company has to protect itself from all possible threats that may jeopardize their

---

<sup>17</sup> In this model we assume that the reward is only available for the first people who reports the bugs.

goal to shift toward a new way of remote operation. As shown in Figure 1, known risks consist of unplanned downtime from known exploits, unplanned downtime from patching failures and planned downtime for patching. Another, often neglected risk is *unplanned downtime from unknown vulnerability exploits*.

For a better assessment of the security threats to Integrated Operations it is crucial to understand the growth of the vulnerabilities black market. An expanding black market for software vulnerabilities might significantly increase the risk of unplanned downtime from unknown vulnerability exploits. The simulations in the previous section suggest that vendors can definitely shorten the duration of the vulnerabilities circulating in the black market.

Now we discuss the alternative to change the nature of the market. In our simulation, we learn that incentives to sell vulnerability findings to vendors may shrink the vulnerability trading in the black market. Making the vulnerability market legal implies a change of the structure depicted in Section 2, Figure 3.

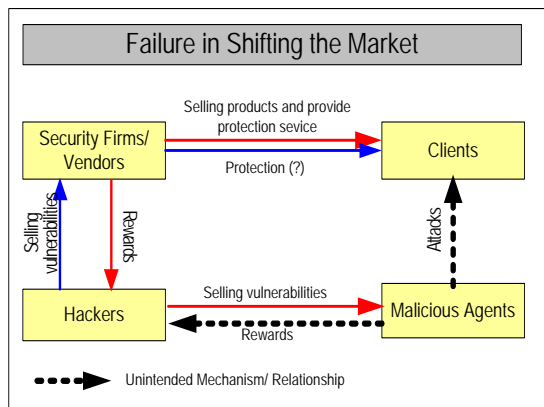


Figure 8  
Failure in Shifting the Market

Although one would hope that this is a change for the better, note that there is also a worst possible scenario when this market structure changes (Figure 8): The hackers might sell the information to both parties: vendors and criminals. The unintended consequence of such change might be a resurgence of the initial structure between hackers, malicious agents, vendors and clients. The outcome might even be worse because hackers would have more economic advantages, while ultimately the

software users still do not obtain a better protection. Our model so far neglects this issue and only considers the options of selling vulnerabilities to the vendors or selling them to malicious agents. However this likelihood should be considered in future model efforts in order to better capture this unintended impact of a legal vulnerability market. There is awareness of this danger, as the disagreement about a recent trend to legalize vulnerability market shows. Kaplan [23] for example states: "This could have insightful implications for organizations and end users, as vulnerability information will be given a financial value that may motivate researchers to sell that information on the open/legal/ free market or on the black market to the highest bidder, rather than disclosing them publicly on mailing lists or websites".

Schechter ignores the issue of how the vulnerability market concept proposes a solution for testers selling vulnerabilities to dual parties. Ozment considers how the auction theory can reduce the possibility of the unknown vulnerabilities circulating in the black market, but he also mentions the possibility of attack to the bidders. Ozment [9] called this problem *resale* and *collusion*. Particularly the resale problem, it is closely related to the vulnerability black market problem. Resale occurs when the testers sell vulnerability reports not only to the producers but also to the black market and perhaps to malicious hackers. They still have chance to advertise vulnerabilities as having been reported, but as-yet unfixed. Buyers could then pay a price equal to their usefulness for a short-lived vulnerability. Ozment [9] is aware that the vulnerability market does not have any real solution to this dilemma; but he is optimistic that the bug auction could decrease the likelihood of resale by reducing the reward for the testers by some fraction if a bug is found to be exploited before the vendors are able to release a patch.

The lessons from the above discussion that the roles of vendors, security firms and other philanthropic organizations or individual researchers for changing the vulnerability market structure seems also important to help reducing exploits from unknown vulnerabilities. Shifting towards a legal market has started—although there are pro's and con's too, including ethical issues. Among them are Kannan and Telang [24]. They argue that vulnerability market-based mechanism – especially an unregulated one, reduce the social welfare of the users. They suggest vulnerability market not follow the traditional market, because the market requires proper policy interventions regarding vulnerability disclosure.

In future research we will explicitly model the risk of unknown vulnerability attacks faced by the company transitioning to Integrated Operations. Understanding this hidden threat better should be relevant for any company relying on computer networks for their primary business. We intend to expand the system dynamics model to describe the intended action of creating legal vulnerability market and the unintended consequences of hackers' behavior for selling their finding to software producers/security company and again, to the black market. There are time delays and feedback relationships in this process that can be explained using system dynamics modeling.

Owing to the conceptual nature of the model our assessment should be considered as a starting point for discussion and the exchange of visions and opinions.

## References

- [1.] Whitman, M.E., *In Defense of The Realm: Understanding The Threats to Information Security*. International Journal of Information Management, 2004. **24**: p. 43-47.
- [2.] Johnsen, S.O., M.B. Line, and A. Askildsen. *Towards More Secure Virtual Organizations by Implementing a Common Scheme for Incident Response Management*. In *Eight International Conference on Probabilistic Safety Assessment and Management (PSAM8)*. 2006. New Orleans.
- [3.] Bouchard, M. *Unknown Attacks: A Clear and Growing Danger*. 2005 [cited; Available from: [http://searchwindowssecurity.bitpipe.com/detail/RES/1136907342\\_223.html](http://searchwindowssecurity.bitpipe.com/detail/RES/1136907342_223.html)].
- [4.] The\_Honeynet\_Project, *Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community*. 2002, Boston: Addison-Wesley.
- [5.] The\_Honeynet\_Project, *Know Your Enemy: Learning About Security Threat*. Second Edition ed. 2004, Boston: Addison-Wesley.
- [6.] Greenemeier, L. *The Fear Industry*. Information Week 2006 [cited 2006 August 20]; Available from: <http://www.informationweek.com/story/showArticle.jhtml?articleID=185301289>.
- [7.] Sutton, M. and F. Nagle. *Emerging Economic Models for Vulnerability Research*. In *The Fifth Workshop on the Economics of Information Security (WEIS)*. 2006. Robinson College, University of Cambridge, England.
- [8.] Schechter, S. *How to Buy Better Testing: Using Competition to Get The Most Security and Robustness for Your Dollar*. In *Infrastructures Security Conference*. 2002.
- [9.] Ozment, A. *Bugs Auctions: Vulnerability Market Reconsidered*. In *Workshop of Economics and Information Security (WEIS)*. 2004. Minneapolis, MN.
- [10.] Anderson, R. *Why Information Security Is Hard, an Economic Perspective*. In *17th Annual Computer Security Applications Conference*. 2001.
- [11.] Böhme, R. *Vulnerability Markets: What Is The Economic Value of a Zero-Day Exploit?* . In *22 C3*. 2005. Berlin, Germany.

- [12.] Böhme, R. *A Comparison of Market Approaches to Software Vulnerability Disclosure*. In *International Conference, ETRICS 2006, LNCS 3995* 2006. Freiburg, Germany: Springer-Verlag Berlin Heidelberg.
- [13.] Akerlof, G.A., *The Market for "Lemons": Quality Uncertainty and Market Mechanism*. The Quarterly Journal of Economics, 1970. **84**(3): p. 488-500.
- [14.] Finjan. *Web Security Trends Report*. 2006 [cited 2006 September 20]; Available from: <http://www.finjan.com/Content.aspx?id=827>.
- [15.] Itzhak. *Malicious Code for Sale*. 2006 [cited 2006 August 3]; Available from: <http://ipcommunications.tmcnet.com/hot-topics/Security/articles/1942-malicious-code-sale.htm>.
- [16.] Schechter, S. *Toward Econometric Models of Security Risk from Remote Attacks*. In *The Third Workshop on Economics and Information Security*. 2004. Minneapolis.
- [17.] Sterman, J.D., *Business Dynamics : Systems Thinking and Modeling for a Complex World*. 2000, Boston: Irwin/McGraw-Hill.
- [18.] Richardson, G.P. and A.L.P. III, *Introduction to System Dynamics Modeling*. 1981: Productivity Press, Portland, Oregon.
- [19.] Randers, J., *Elements of the System Dynamics Method*. 1980, Cambridge, Massachusetts: The MIT Press.
- [20.] Ellison, R.J. and A. Moore. *Trustworthy Refinement Through Intrusion-Aware Design (TRIAD)*. 2003 [cited 2003 September 10]; Available from: <http://www.cert.org/archive/pdf/03tr002.pdf>.
- [21.] Strauss, J. and R. Frost, *Marketing on the Internet*. 1999, Upper Saddle River, New Jersey: Prentice Hall.
- [22.] Rogers, M.K., *A Social Learning Theory And Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study*, in *Department of Psychology*. 2001, University of Manitoba: Winnipeg, Manitoba.
- [23.] Kaplan, D. *Threats for Sale*. SC Magazine 2006 [cited 2006 August 4]; Available from: [www.scmagazine.com/us/news/article/556843/threats-ale/](http://www.scmagazine.com/us/news/article/556843/threats-ale/).
- [24.] Kannan, K. and R. Telang, *Market for Software Vulnerabilities? Think Again*. Management Science, 2005. **51**(5): p. 726-740.
- [25.] Johnsen, S., et al., *CHECKIT – A Program to Measure and Improve Information Security and Safety Culture*. International Journal of Performability Engineering, 2007. **3**(3): p. 271-286.

## Appendix

Integrated Operation works by transmitting “live” data from offshore to onshore “control rooms”, where the department onshore analyses data and collaborates with the same department offshore. Oil companies use these ‘control rooms’ onshore to run the work processes occurring offshore. An important goal of *Integrated Operations* is to safely access and support offshore processes and data from wherever the employees are located.

*Integrated Operations* is a gradual process to transform traditional process with originally self-sustainable fields offshore to integrated centers and real time communication. Ultimately Integrated Operations will provide 24/7 virtual centers and digital services. Daily operational decisions that only obtain limited onshore support in traditional operations would be improved by collaborative decision-making of teams onshore and offshore. Offshore gets continuous

support from onshore and in reverse onshore gets real-time information about operations offshore. As Integrated Operations matures, several work processes and decision are automated, and collaboration decision are made by people in operators onshore support centers and vendors as well as expert centers.

The aim of Integrated Operations is to increase the production approximately by 10% and to reduce costs by 30%, and to improve the collaboration between offshore and land-based personnel. The important advantages of Integrated Operations concerning increase in safety are: faster detection of dangerous situations, reduce exposure to risks for offshore personnel, better use of competence, be able to draw up more oil, faster access to expertise in relation to critical events, improved integrations across trade, location and organization.

The technology used in process control systems (PCS) and supervisory control and data acquisition (SCADA) systems is changing from proprietary closed systems to standardized IT systems integrated in networks that may be connected to internal networks and to the Internet [25].