Cost Tradeoffs For Information Security Assurance

Ritesh Kumar Tiwari Kamalakar Karlapalem
Center for Data Engineering, International Institute of Information Technology, Hyderabad, INDIA-500019
ritesh@students.iiit.net, kamal@iiit.net

ABSTRACT

Information security is important in proportion to an organization's dependence on information technology. Security of a computer based information system should protect the *Confidentiality*, *Integrity* and *Availability* (*CIA*) aspects of the system. With the increasing dependence of business processes on information technology, the number of attacks against CIA aspects have increased manifold. Since achieving perfect security is monetarily and practically infeasible, organizations are using risk management concepts to forego perfection and instead making tradeoffs in pursuit of security goals. In this paper, we focus to analyze such tradeoffs in terms of *investment costs* and *opportunity cost* (from perspective of defender and attacker respectively).

1. INTRODUCTION

Information security is hardly a new concept. Practice of information security continues to be an evolving endeavor where technological advances both help and hinder its growth. From an organizational centric view, loss of information could lead to *Direct losses* (quantified in terms of dollar losses) and *Indirect losses* (e.g. loss of customer faith[1], damage to reputation etc.). As Blakley et.al. [1] points out, the basic problem with information security is that it focuses more on reducing the probability of occurrence of an adverse event, rather than on reducing its consequences. So the main aim of any security risk management techniques should be to optimize the cost of risk to business, rather than on minimizing the probability of occurrence of adverse event. From the perspective of risk management, security risk can be defined as:-

Security risk = (security breach rate) x (average cost per attack).

As Schechter [2, 3] points out, Adversary Ranks (number of potential adversaries), Adversary Incentives (how valuable attack appears to potential adversaries), Adversary Attack Risk, and Adversary Cost of Attack are four parameters likely to affect the rate at which system is attacked. Apart from the above, we believe that popularity of a business (or a server) is also an important parameter to be considered (as number of attacks on well known web servers are much higher when compared to the ones on not so well known servers).

Every year, enormous amount of money and effort is invested in finding, publishing, and fixing vulnerabilities in software products. Such vulnerabilities are detected by either Red-teams (amateur researchers) who sell their findings to company in exchange of money (called as White Hat Discovery - WHD) or by hackers who exploit them for launching attacks (called as Black Hat Discovery – BHD). Once vulnerability is found out, it is publicly disclosed and patches are rolled out by company for public use. It has been found that public disclosure of vulnerability itself triggers an enormous rate of public exploitation (fig. 1)[2] because attack scripts are written which are freely available for not so technically sound hacker base [14].

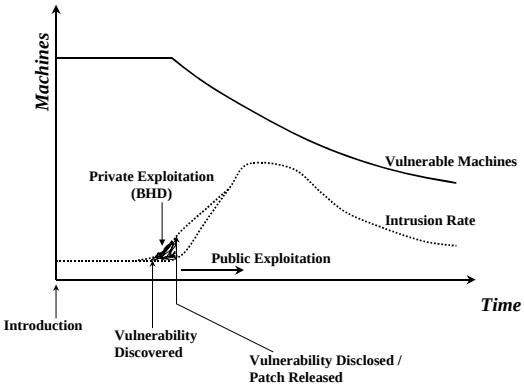

Fig. 1 Vulnerability Disclosure vs. Intrusion Rate

Since the stability and correctness of a patch cannot be guaranteed during its release, when to apply patches to a system is a tough problem [5]. In this paper, we focus on above issues with a cost based approach consisting of both opportunity cost and investment costs.

2. RELATED WORK

Gordon et.al. [6] propose an economic model that determines the optimal amount to invest for protecting confidentiality, availability, authenticity, non-repudiation and integrity of information. They use a version of *ALE* (annual loss expectancy) that is modified for situations where at most one successful breach will occur. Kevin Soo Hoo [8] uses safeguard efficacy to weight the benefits of different security policies. Formally speaking, net benefit for K^{th} security policy P_k is defined as:-

$$Net\ Benefit_k = (ALE_0 - ALE_k) + Added\ profit_k - Added\ cost_k$$

The main limitation of this model is its over estimation in risk reduction in case of using those safeguards, which substitutes each other in functionality.

Schechter [2] in his doctoral dissertation develops a formal model for economic measure of software security strength with respect to threat scenarios. He also proposed a regression and probabilistic framework for anticipating new threats. Meadows [9] proposed cost based framework based on *attack cost* and *protocol engagement cost* for resisting denial of service attacks against protocols. Jelen et. al. [11] discuss the role of assurance in risk management with emphasis on uncertainty in risk measurement. Kannan et. al. [12] discusses an active market based mechanism for vulnerabilities (considering both white hat and black hat discovery) and characterize it in terms of both

[1] Many customers now days hesitate in responding to promotional e-mails due to fear of *Phishing Attacks.*

[2] This figure is derived from fig. 1 and fig. 2 of [14].

unregulated markets (where the informediary leaks out vulnerable information) and regulated market.

Various formal verification tools like $Mur\varphi$ have been developed for automated formal verification of cryptographic protocols. Since real world risk analysis is both computationally complex and intensive, need of such automated tools that allows reasoning on attacks and helps in building security decisions is highly desirable. Hamdi et.al. [13] address the problem of automating risk management. They propose an algebraic approach for modeling risk management projects and of proving the properties in risk management signature.

In short, a strategy to manage security is essential. Such a strategy should be based on an ongoing cycle of risk management and should treat the entire business processes inside organization in a unified framework. It should identify significant risks, clearly establish the responsibility for reducing them, and ensure that risk management remains effective over time.

3. OUR APPROACH

We have used following symbols used throughout the paper -

V_i	Vulnerability *i* where *i* = 1, 2, …, n
S_j	Safeguard *j* where *j* = 1, 2, …, n
$C(S_j)$	Investment Cost. cost of implementing safeguard S_j
$R(S_j)$	New profits enabled by adoption of safeguard S_j
$F_0(V_i)$	Initial estimate of frequency of attacks targeting V_i
$D_0(V_i)$	Initial estimate of damage resulting from attack targeting V_i
$R_a(V_i)$	Return value for an attacker of a successful attack targeting vulnerability V_i

3.1 Semantics of Opportunity Cost

Opportunity cost $C_a(V_i)$ for an attacker can be defined as cost borne by attacker for exploiting vulnerability V_i. An attacker usually will not prefer to attack a target unless:-

i. The return value[3] $R_a(V_i)$ of exploiting vulnerability V_i is more than the opportunity cost $C_a(V_i)$ i.e. $R_a(V_i) > C_a(V_i)$, and

ii. The probability of an attempt being successful are high (otherwise it will cause some opportunity cost to attacker with zero returns)

To successfully exploit vulnerability V_i, attacker has to execute series of steps $\{E_1^{a_i}, E_2^{a_i}, \ldots, E_n^{a_i}\}$. Usually there exists a partial causal relationship in between these sub steps, i.e. $E_1^{a_i} \prec E_2^{a_i} \prec \ldots \prec E_n^{a_i}$. Successfully executing every sub step will incur a cost on attacker called as protocol engagement cost. If $C_a(E_j^{a_i})$ represents protocol engagement cost for step E_j, then the *opportunity cost* $C_a(V_i) = \sum_{j=1}^{n} C_a(E_j^{a_i})$.

Based on technical expertise of attacker, protocol engagement cost may vary. So treating opportunity cost as a deterministic value is a wrong approach. We can only have an approximate value for opportunity cost. Success ratio of attacker exploiting vulnerability V_i can be defined as-

$$success\ ratio_a(V_i) = \frac{\text{Number of successful attacks targeting } V_i}{\text{Total number of attempts targeted for } V_i}$$

3.2 Semantics of Investment Cost

The purpose of security investment is to lower the probability that information system of organization will be breached. In other words, an attacker will have to invest more efforts to fetch the same information as compared to the case when safeguard was not there, i.e. $C_a(V_i, S_j) >> C_a(V_i)$. So the net profit value of information that attacker is trying to gain by exploiting vulnerability V_i is reduced to a low level. We believe that treating security investment in terms of lowering the probability of attack is at a coarse level and should be treated in much finer level. For example, when a patch S_k with cost $C(S_k)$ is applied for stopping attacks that exploit vulnerability V_k, then it is useful only if it reduces the number of attacks targeting V_k to zero, otherwise the investment has no utility (i.e. no return value).

In order to stop a security breach (consisting of steps $E_1^{a_i}, E_2^{a_i}, \ldots, E_n^{a_i}$) and targeting vulnerability V_i, let the safeguard S_i execute steps $E_1^{s_i}, E_2^{s_i}, \ldots, E_n^{s_i}$ to protect the system from successful attack. Let $E_n^{a_i}$ denote the last event executed by attacker whose successful execution means the attack targeting to exploit V_i is successful. Since executing $E_1^{a_i}, E_2^{a_i}, \ldots, E_n^{a_i}$ will incur protocol engagement cost to attacker, an *ideal* protection mechanism be such that it lures attacker to waste his resources in protocol engagement and block the critical step (i.e. $E_n^{a_i}$) at which the attack will be successful. An inherent requirement of this approach is that protocol engagement for safeguard in initial stages should be low.

In order to achieve this *ideal* goal, the safeguard should be able to infer from execution of $E_1^{a_i}, E_2^{a_i}, \ldots, E_{n-1}^{a_i}$ that whether someone is trying to breach into or it is a normal access

[3] We assume that there are no "*just for fun*" attackers as the return value of attack for these attackers is immaterial.

pattern. If it is an attempt to break into the system, then $E_n^{a_i}$ should be blocked. This is where the current generation of security products fail. Most of the systems simply allow or stop an event. There is no mechanism to take into account the previous access and execution history to decide (or infer) whether the series of steps constitute an attack pattern or a normal pattern (Though research in area of Anomaly Based Intrusion Detection systems and Adaptive access control systems is going, but it is still in its infancy).

A notable attempt to increase protocol engagement cost of attacker is to implement *TCP/IP fingerprint scrubber* [15] on web server. High-speed high bandwidth servers with static IP address are prime targets of attack. They are then later used as stepping-stones for launching massive attacks. Since the primary phase of attack begins with probing operating system (and its version) that is running on target system, such scrubbers misguide the attacker thereby creating a large search space, which is pretty costly for an attacker to explore.

In short, from global perspective, the safeguard developed should be such that they not only protect the owner, but also increase the cost of protocol engagement to the attacker. This approach will be a leap forward attempt in achieving the vision of globally secure Internet.

3.3 Analysis of Real World Problems with Investment Cost and Opportunity Cost

Recent security surveys [27, 28, 29, 30, 31] reveals that *Virus/worm attacks* are most prevalent followed by *Insider Attacks* and *System penetration attacks*. The survey also reveals that 99% of the organizations surveyed use Antivirus Software, 98% use Firewalls, 71% used Server based Access Control Lists, 68% used Intrusion Detection system, and 64% encrypted the data during transit.

3.3.1 Approach for Combating Virus/ Worm/ Denial of Service Attacks

A canonical question that comes in mind is that when 99% of organizations have Antivirus software and firewalls, then why virus and worm attacks are so prevalent. The basic problem starts with security survey statistics itself. Knowing that an organization uses anti-virus software is of minor importance compared to uncovering information about the number of systems that have anti-virus software installed, whether the anti-virus software is continuously running, or the frequency with which the virus definitions are updated. In reality, a big problem is that anti-virus definitions are not updated very regularly. Regularly updating anti-virus software with latest virus definitions can solve this problem to a great extent. Some worms target vulnerability in specific operating system/ server software using specific port numbers. In such cases there are two options for an administrator:-

(i). Block the port and service being exploited by worm (if they are not used by the organization), and apply the patches later (after verifying the correctness of patch). Blocking service and port will incur approximate zero investment cost to organization and trying to exploit the blocked service high incur opportunity cost to adversary. So the system is secure. Later on patching the system (with safeguard S_j) will incur low investment cost to organization ($C_{patch}(S_j) \rightarrow low$) and opportunity cost for adversary will remain high.

(ii). When service and port cannot be blocked, then in such cases, either the administrators can take an optimistic approach (assuming patch will work correctly) and apply patches, or can defy from not applying patches (assuming that patch may not function correctly and may induce other errors). Usually the probability of a patch being bad is less than the probability of being a victim of worm attack (We assume that these machines have high bandwidth Internet connectivity and static IP addresses). Once these machines get infected, the worm can propagate by itself inside the organization in few minutes. If affordable for an organization, then the patches should first be tested on standby systems and then be applied on front-end systems. If that is not affordable, then the patch should at least be installed on those systems that have direct high-speed connectivity to Internet and have static global IP address.

Four necessary conditions that must be met for an infected host to be able to infect an uninfected host can be described in terms of *Targeting, Host Visibility, Vulnerability,* and *infectability* [24]. A promising way to check propagation of worm is by making visibility opaque. This can be done by blocking unused ports (services) and installing fingerprint scrubbers on front-end servers.

In worm attack, the initial probing cost is borne by attacker. Once rootkits and payload are installed on server, from then onwards the probing cost is borne by servers (or intermediate machines) and not directly by the attacker. Since many network parasites employ social engineering attacks (e.g. e-mails containing luring subject and attachment titles), employee awareness in such cases can prove to be very important.

We prefer to include denial of service attacks in this section because many of the worms are intended for launching denial of service attacks. Network Denial of Service (DoS) has became a widespread problem on Internet. Availability requires that computer system remain functioning as expected without degradation in Quality Of Service and resources remain accessible to legitimate users. While several measures like load balancing, resource throttling, dynamic resource pricing, packet filtering etc are proposed in literature, there exists no solution for completely protecting a system against DoS attack. One viable solution is to design protocols such that during initial stages, the cost of interaction with the protocol is high for the connection initiator rather than the server. This is so because most of the Denial of Service attacks exploit IP address-spoofing techniques.

Let $E_1^I, E_2^I, \ldots, E_n^I$ be the protocol engagement steps executed by Initiator (a legitimate or a malicious node) and $E_1^S, E_2^S, \ldots, E_n^S$ be the corresponding protocol engagement steps executed by the server. For a protocol to be resistant against Spoofing DoS attack (e.g. State exploitation *SYN* attacks against TCP protocol) and Computational Denial of service attack, the cost of executing protocol be such that $C(E_1^S) =$ *minimal* (i.e. $C(E_1^S) \rightarrow 0$) and for first few protocol steps $C(E_1^S) < C(E_1^I), C(E_2^S) < C(E_2^I), \text{---}, C(E_n^S) < C(E_n^I)$ where n represents few initial execution steps of the protocol.

The cost $C(E_i)$ here is measured cumulatively in terms of CPU cycles used and memory used for storing intermediate states.

3.3.2 Approach for Combating Insider Attacks

An attack launched by current or former employee/contractor of an enterprise against the employing enterprise itself is known as Insider Attack. Malicious Insiders pose a substantial threat because of their knowledge about employer's information system architecture, and their ability (access rights) to bypass existing physical and electronic security measures through legitimate means. The primary aim of a malicious insider is to hide his/her malicious activity and sometimes the consequences of attack also. Though number of such attacks is low, but the consequences of such attacks are detrimental for the organization [17]. The main problem with insider attacks is that they are hard to be detected because they span over a long period of time, and the cost of both consequences and of launching the attack has to be borne by same organization.

How to predict (or better say detect) and mitigate such attacks is an open area of research. Most of the security solutions, which are efficient in checking remote attacks (i.e. outside attacks) fails in insider attack scenario. In case of outsider attack, the risk of being caught is immaterial to attacker because he is geographically far apart and moreover his location is vague (because most of these attacks are launched by compromised machines that act as stepping stones for the attacker). But in insider scenario, if malicious activity is detected then the risk of being caught and prosecuted are high. So it is the risk and not the cost of efforts (or resources) that deter the insider from launching an attack.

One approach to tackle problem of attacks from malevolent insiders is to classify sensitivity of information (and systems) appropriately[4] and suitable level of protection be applied at each level. Usually the prime targets for a malevolent insider are financial system of organization or those mission critical system whose damage will cause tremendous losses to organization. For such systems containing critical information, applying multiple level of defense (defense in depth) is a better option. Preferably those safeguards should be deployed which create logs for each interaction that takes place with them. Careful analysis of *attack graph* targeting such critical information will enable us to know avenues from where the information can be compromised. So the safeguards preferably should be those, which partially overlap in checking those avenues of compromise.

Of course the above-mentioned approach of defense in depth with user profiling is very costly to implement and maintain, but that is the only way for an organization to protect its mission critical information, else such attacks may prove fatal to overall existence of organization.

3.3.3 Approach to Combating System Penetration Attacks

As such, penetration attacks do not have specific characteristics like virus (worms) and insider attacks. Broadly speaking, penetration attack targets technical, configuration and operational vulnerabilities in operating system running on target, applications running on target, firewall rule base, scanning router, security policy etc. The aim of attacker is to exploit any of the vulnerabilities that might exist in target system so as to gain access into target system for obtaining sensitive information or for using it as a stepping-stone.

The most common technique to overcome penetration attack is to employ red teams for performing penetration testing of organization information infrastructure. The basic aim of penetration testing is to find design weakness, technical flaws and vulnerabilities in system design and policy implementation. Organizations that have employed penetration testing using *Black box* (with no prior knowledge of target system and network infrastructure) or *Crystal Box* (with complete knowledge of network technology and target configuration) have resisted many penetration attacks. Penetration testing does not guarantee perfect security. It only let us know the common errors and vulnerabilities in currently deployed system. Once these errors are rectified, the cost of breaking into the system for a hacker will usually[5] be pretty high.

Another common tool used by organizations to increase complexity of penetration attack is Network Address Translator (NAT) that hides the internal network structure from outside world. Encryption of sensitive information during storage is also cited as effective means for significantly increasing the cost of gaining secrets for the attacker. Since most of the penetration attempts are black box based, network usage monitoring (e.g. packet drops etc.) and application monitoring (false login attempts, trying to use privileged directories and commands etc.) can prove to be effectual in dealing with such attacks. Honeypots with luring system account information and directory names have also been deployed for finding attack pattern of attacker. But they are useful only when attacker interacts with them, else they are a financial burden on organization. All these techniques are deployed practically, but they do not increase attackers opportunity cost significantly.

Data obfuscation needs a special mention in this regard. Suppose a sensitive file F is to be protected from illegal access. If this file is stored on a single machine and that machine is subverted, then attacker can gain the entire sensitive information. But if the file F is divided into k chucks (i.e. $F_1, F_2, F_3, \cdots F_k$) and these chucks are stored not on one place but throughout the network, then the search space for attacker will increase tremendously and so is his cost of accessing the file. Since the probability of intrusion detection by IDS when attacker attempts to attack large number of machines on network is very high, such attacks can easily be detected and blocked. In such a scenario, the opportunity cost for attacker is tremendously high, the investment cost for organization is low, and the chances of a successful breach of confidential information are minimal. One practical application using a variant of the above approach is done by Dragon et.al [20] where they have hidden chunks of confidential file in a very large single file (of terabyte size) for preventing insider attack on sensitive data.

4. CONCLUSION AND FUTURE WORK

As was mentioned in Grand Challenges [26], "*we cannot manage the risk if we cannot measure the risk*". This is because if we do not have accurate measure, then either we will under

[4] Organizations should make a careful assessment that what losses will they suffer if critical information (or system) is lost (or damaged).

[5] People have different programming and hacking skills, and based on these skills and their experiences, they can have varying opportunity cost.

protect or over spend. Today we have no way to differentiate whether software (system) costing $500 better suits our security needs or a software (system) costing $600. We have no metrics to accurately determine the return value of investment that we are making for securing the information. So an open research area is to develop technologies and metrics so that the protection level that a new system (software) provides can be quantified as per different aspects.

Another main hurdle is that still we do not understand full nature of causes that creates IT risks[6]. We do not understand the emergent behavior of viruses, worms, attack patterns and of course vulnerabilities. This is still an unexplored area and lot of work is needed so that mathematical models for risk prediction can be formulated. Security risk will be poorly understood until a much better job of quantification of losses from security breaches is done. We believe that security surveys when conducted at finer level of detail will reveal better and more accurate information regarding the causes of failure and incurred losses. So the need of hour is to come up with a non profit organization (society) consisting of members from industry, academia, research institutions, where the causes of security breaches and related losses can be shared and discussed (with anonymity) so that better hypothesis and mathematical models can be designed to tackle this grand research challenge.

5. REFERENCES

[1] Bob Blakley, Ellen Mc. Dermott, Dan Geer, "Information Security is Information Risk Management", Proceedings of New Security Paradigm Workshop 2001. pp. 97-104.

[2] Stuart E. Schechter, "Computer Security Strength & Risk: A Quantitative Approach", Ph.D. Thesis, Harvard University, May 2004.

[3] Stuart E. Schechter, "Toward Econometric Models of the Security Risk from Remote Attacks", IEEE Security & Privacy Magazine, vol 3(1), 2005. pp. 40- 44

[4] Hilary K. Browne, William A. Arbaugh, John McHugh, William L. Fithen, "A trend analysis of exploitations", In Proceedings of the IEEE Symposium on Security and Privacy, May 2001. pp. 214–229

[5] Steve Beattie, Seth Arnold, Crispin Cowan, Perry Wagle, Chris Wright, Adam Shostack, "Timing the application of security patches for optimal uptime", USENIX Systems Administration Conference (LISA 2002), 2002. pp. 233-242

[6] Lawrence A. Gordon, Martin P. Loeb, "The economics of information security Investment", ACM Transactions on Information and System Security, Vol. 5(4), Nov 2002. pp. 438–457

[7] Ross J. Anderson, "Why information security is hard: An economic perspective", 17th Annual Computer Security Applications Conference, Dec 2001. pp. 358

[8] Kevin J. Soo Hoo, " How Much Is Enough? A Risk-Management Approach to Computer Security", PhD thesis, Stanford University, June 2000.

[9] C. Meadow, "A Cost Based Framework for Analysis of Denial of Services in Networks", Journal of Computer Security, Vol 9, No. ½, , 2001. pp. 143-164

[10] George F. Jelen, "A New Risk Management Paradigm For INFOSEC Assessments and Evaluations," IEEE 11th Annual Computer Security Applications Conference, 1995. pp. 261-267.

[11] George F. Jelen, Jeffery R. Williams, "A Practical Approach to Measuring Assurance", Proceeding of the 14th Annual Computer Security Applications Conference, 1998

[12] Karthik Kannan, Rahul Telang, Hao Xu, "Economic Analysis of the Market for Software Vulnerability Disclosure", Hawaii International Conference on System Sciences, Jan 2004.

[13] Mohamed Hamdi, Noureddine Boudriga, "Algebraic specification of network security risk management", ACM workshop on Formal methods in security engineering (FMSE), 2003. pp. 52-60.

[14] E. Rescorla, "Is finding security holes a good idea?", Workshop on Economics and Information Security 2004, May 2004.

[15] M. Smart, G.R. Malan, F. Jahanian, "Defeating TCP/IP Stack Fingerprinting", 9th USENIX security symposium, 2000. pp. 229-240.

[16] Adam Young, Moti Yung, "Cryptovirology: extortion-based security threats and countermeasures", Proceedings of IEEE Security and Privacy, 1996. pp. 129-140

[17] Gurpreet Dhillon, Steve Moores, "Computer Crimes: Theorizing about the enemy within", Computer & Security, vol 20(8), 2001. pp. 715-723

[18] A. Jøsang, D. Bradley, S.J. Knapskog, "Belief-Based Risk Analysis", Australasian Information Security Workshop (AISW), January 2004.

[19] Stuart Schechter, Michael D. Smith, "How Much Security Is Enough to Stop a Thief?: The Economics of Outsider Theft via Computer Systems and Networks", Financial Cryptography 2003. pp. 122-137

[20] David Dragon, Wenke Lee, Richard Lipton, "Protecting Secret Data from Insider Attacks", To Appear in Proceedings of Financial Cryptography, 2005.

[21] F. Harmantzis, M. Malek, "Security Risk Analysis and Evaluation," Proc. IEEE International Conference on Communications (ICC '04), 2004. pp. 1897-1901

[22] Howard Kunreuther, Geoffrey Heal, "Interdependent Security: The Case of Identical Agents", National Bureau of Economic Research Working Paper No. 8871, April 2002.

[23] Andrew M. Odlyzko, "The Unsolvable Privacy Problem and Its Implications for Security Technologies", Australian Conference on Information Security and Privacy, LNCS-2727, 2003. pp. 51-54

[24] Dan Ellis, "Worm anatomy and model", Workshop on Rapid Malcode, ACM Conference on Computer and Communications Security, 2003. pp. 42 - 50

[25] Wenke Lee, Wei Fan, Matthew Miller, Salvatore J. Stolfo, Erez Zadok, "Toward Cost-Sensitive Modeling for Intrusion Detection and Response", Journal of Computer Security, vol. 10(1/2), 2002. pp. 5-22

[26] CRA Grand Research Challenges in Information Security and Assurance, 2003. (http://www.cra.org/Activities/grand.challenges/security/home.html)

[27] CSI/FBI - Computer Crime and Security Survey, 2004.

[28] Ernst & Young – Global Information Security Survey, 2004.

[29] PriceWaterHouseCoopers – Information Security Breaches Survey, 2004.

[30] CSI/FBI - Computer Crime and Security Survey, 2003

[31] Ernst & Young – Global Information Security Survey, 2003.

[6] Sometimes the attack evolved weeks after when the vendor released patches. Notable examples are Nimba, Code-Red and Blaster.