Cyber Security Economics

Benedict Chen, Girish Dhoble, Manish Choudhary, Nikita Gupta and Sahil Chadha
Georgia Institute of Technology

ABSTRACT

Information and communications technology has influenced all critical infrastructures including energy, transportation, health, education and trade. Due to persistent attacks on critical infrastructures, cyber security has gained momentous attention recently. The incentives for a player in the cyber ecosystem decide the level of security provided and sometimes result in externalities getting created in the ecosystem. As the arms race between the cybercriminals and businesses is evolving, lack of a secure and robust cyber infrastructure is in large part the direct result of a failure to recognize and address the incentives and the technological, social and economical factors underlying them. Cyber economics plays a key role in the decisions and motivation of software vendors like Microsoft and also of the cyber criminals like botmasters.

INTRODUCTION

Many aspects of our lives rely on the internet and computers including communications, transportations, government, finance, medicine, education etc. Cyber Security involves protecting the vast amount of personal information and systems we rely on every day, whether at home, work or school. Economics of security has recently become a fast moving discipline. Due to persistent reports on critical computer being compromised and hackers emptying bank accounts, cyber security has grabbed attention of many across the world. Many problems plaguing cyber security are economic in nature. Systems often fail because the organizations that are responsible for their protection do not bear the full cost of failure. Policies should be employed in such a way that the parties who are responsible for the protection should have an incentive to do so. Hence, the economic perspective is necessary for understanding the state of cyber security as well as improving it moving forward.

In this paper, the cyber security economics is described which signifies the trade-off between the cost of securing the asset and their worth as per the business model. We describe the three crucial economic barriers to improving cyber security: Misaligned Incentives, Information Asymmetry and Externalities. Finally, we present a case study describing the evolution of the Microsoft Windows operating system from security point of view. The case study describes the economical aspects from both the perspectives: good players and bad players in the market. It also explains the disincentives involved for investing in the security of a product.

RELATED WORK

Cyber economics is a vast subject and there have been a lot of work published in this field. The work in this paper has been influenced from some of these intensive papers. A paper by Eeten et. al. on malware oriented cyber economics discusses about ecosystem, the various players in the ecosystem and the externalities created by them, and also presents direct and indirect costs involved in providing security. Moore discussed about various incentives for investing in security, cyber threats, presented some open problems and suggested some solutions. Anatomy of a Botnet, a paper by Fortinet, discusses about cyber economics from the perspective of cybercriminals. It focuses on botnets, the most efficient tool for monetizing the cyber crimes by providing crime-as-a-service, the different purposes for which botnets can be used, the profit margin that botmasters/cybercriminals get as well as the costs involved in setting up a botnet.

In addition, some good work has been published in the form of articles on blogs which present some interesting facts and figures, related to cybercrime and cyber economics.

ECOSYSTEM OF CYBER SECURITY ECONOMICS

Here, in this section different actors/ players and different activities which are involved in cyber security are presented and how they affect the economics of other players involved. Major players involved in cyber security ecosystem are: Software vendors, Hardware vendors, Internet service providers, Users and applications.

A. Criminal activity

An activity is the one whose motive is to create security vulnerability in the ecosystem for making profit. People behind these activities can be anyone Hackers, Government agencies or cyber criminals.

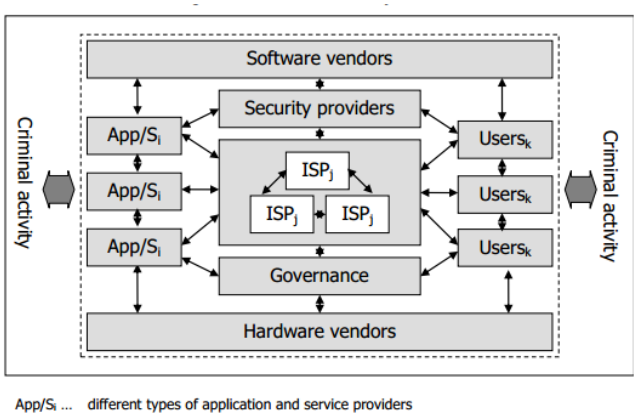

Figure 1: [1]

B. Vendors

These can be hardware vendors or software vendors. If any security breach happens on their side the whole system gets affected and security of every other player in the ecosystem gets affected by it. They will then unnecessarily need to spend extra money to secure their parts as well. Vendors will need to spend extra on patching their product and deploying that patch.

C. Security information provider

Every business small or big is in constant need of security information to asses risk to their product or business. Hence security information providers are hired. Business organizations need to spend extra money on hiring specialized individual for security information. This affects their budget and every other actor/player related to the business ecosystem is affected. If security information providers calculate a wrong estimate for security budget then whole ecosystem suffers because of a single wrong decision.

D. Users

If security is exploited in the ecosystem, so until the patch is created individual users need to secure themselves individually. This affects the economics of the ecosystem and more money needs to be spent on securing the individual users. If individual users are affected by any virus trojans etc, then other players connected with these users will also be at a risk hence users also need to have a security mechanism on their side in addition to the entire network.

ECONOMIC BARRIERS TO IMPROVING CYBER SECURITY

In today's world four of the most prescient threats to cyber security are online identity theft, industrial cyber espionage, critical infrastructure threat and botnets. Each of these threats posses' different technical characteristics and constraints. However, there are some commonalities in terms, as specified by Moore in Introducing the Economics of Cyber security: Principles and Policy Options [2], of the economic barriers inhibiting optimal levels of security investment.

A. Misaligned Incentives

As the term suggests, the incentives of the person who benefit from security protection are not aligned with the incentives of the person or firm responsible for protecting the system. Solutions exist for many of the threats introduced by casual adversaries, but these solutions are not widely used because incentives are not aligned with objectives and resources are not correctly allocated. For example, electric companies have upgraded their control systems to run on the same IP infrastructure as their IT networks which resulted in high efficiency gains. But from another perspective, these changes leave the systems more vulnerable to failures and attacks making the society to suffer in case of outrage. In such cases, risks are allocated poorly.

Perfect security is not possible which implies that there exists an optimal level of insecurity where gains from the efficient operation outweighs any reductions in risk brought about by additional security measure. However, the party making the security efficiency trade off is not the one who loses when attack occurs which makes misalignment inevitable for many information security decisions. Secure practices must be incentivized if cyber security is to become ubiquitous.

B. Information Asymmetry

Information asymmetry means lack of reliable data among the players which prevent them from making the right decision about the investment in security of the system. For example, the vendors developing security softwares are unwilling to invest in security measures as the buyers refuse to pay a premium for protection. Hence, security companies are not pressured to bring new technologies in the market against substantial threats. Hence, the lack of reliable data on the costs of information insecurity makes it difficult to manage the risk. From another perspective, this gives an extra advantage to the attackers who can get into the system due to lack of right defences for ideal protection. Ill-informed consumers and businesses are prone to invest in not-so-beneficial solutions if they do not possess an accurate understanding of threats and defences due to information asymmetry.

C. Externalities

The security measures undertaken by an individual have side effects on other's security. For instance, a secure operating system is more difficult to develop applications for which forces the operating system vendors to

compromise on security until market dominance has been achieved. Likewise, the first mover's advantage explains why insecure software is readily pushed to the market giving rise to perpetual "beta" versions of the software rather than spending time on its security. Insecurity creates negative externalities which can be explained in the scenario where a compromised computer that has been recruited to botnet can pollute the internet harming others in the network as described in [3]. But the private risks facing utilities are less than the social risks, which results in underinvestment in the protection of social risks as expected. From the perspective of the botnet master, this could result in the growth of its network due to the negligence of the user of the compromised system.

CYBER SECURITY ECONOMICS FROM THE ENTERPRISE: THE MICROSOFT CASE STUDY

Management teams in large enterprises and corporations are tasked with the challenge of balancing the allocation of resources towards cyber security and the other immediate needs of the company. The quantification of risks in a potential cyber-attack is complex, as it is hard to place a dollar value on intangible constructs such as compromised data and the loss of reputation. What then, governs their spending strategies in cyber security? For the case of Microsoft, we examine how decisions are influenced by company culture and the top-down driven push from its leaders.

Prior to the launch of Windows XP Service Pack 2 in 2004, Microsoft focused primarily on innovation and the delivery of fully featured products. The inclusion of added features and functionalities in product launches overshadowed the requirements of incorporating security into the design of their products. This led to a series of high profile attacks on its software between 2001 and 2003. Prominent examples would include the Code Red, Slammer and Blaster worms. This generated a huge public outcry and a loss of confidence in the quality of Microsoft products. The negative publicity prompted its leaders to re-evaluate its position on the need for a security-centric approach in the design of its applications.

The launch of the Security Development Lifecycle in 2004 signalled a shift in Microsoft's willingness towards investing in stronger software security for their commercial applications. This was the culmination of Microsoft CEO, Bill Gates' grand vision for the adoption of a company-wide, security-centric approach in the software development process, as outlined in his 2002 "Trustworthy Computing" memo [6]. While embarking on such an approach would result in higher expenditures, Microsoft had deemed it necessary for two reasons. Firstly, they were of the opinion that maintaining the good reputation of the company would be of the foremost priority. In addition to this, they had assessed that it was more cost effective to put in resources in fixing potential application bugs during development as compared to coming up with patches for vulnerabilities uncovered after the launch of the software. This is a claim which has been substantiated by NIST [7].

Microsoft reports a vast reduction in the amount of vulnerabilities uncovered in software developed after the launch of the Security Development Lifecycle, as indicated by the Microsoft SQL Server 2005 case study [7]. Their commitment towards security was further enforced with the launch of security strong products such as Windows Vista in 2007, as well as its successors.

THE UNDERGROUND ECONOMY OF CYBERCRIME

The economical aspects with respect to good players in the market have been discussed above. But, the relationship between cybercrime and the involved economical aspects is equally important. Cybercrime refers to the illegal activities undertaken by criminals for financial gain, which exploit vulnerabilities in the use of the Internet and other electronic systems to illicitly access or attack information and services used by citizens, business and government.

A cyber criminal weighs benefits and costs to make decision about engaging in a crime. A cyber crime is committed if $M_b + P_b > O_{cp} + O_{cm} * P_a * P_c + M_c$ where, M_b is 'monetary benefits of committing crime', P_b is 'psychological benefit of committing the crime, O_{cm} is 'Monetary opportunity costs of conviction', O_{cp} is 'psychological costs of committing a cybercrime', P_a is 'probability of arrest', P_c is 'probability of conviction' and M_c is 'monetary cost of committing the crime'[4]. Thus, return on investment and the risk involved are the most important factors driving cyber crime.

Some of the ways to monetize cyber crime are DDoS(extortion), spamming, click fraud, scamming, phishing, pharming, installing scareware and harvesting account details. The most efficient and effective way to launch these attacks is through Botnet infrastructure. A botnet, or zombie network, is a network of thousands or even millions of machines that have been infected with malware, putting them under the remote control of criminals. Because of the high value of financial gains by using botnets, they are used directly by botmasters or rented out. Botmasters (those who architect, harvest, and manage botnets) are involved in many operations related to Crimeware as a Service (CaaS). Notable activities associated with botnets and their impacts on cyber economics are as follows.

A. Denial of Service

An unscrupulous entrepreneur can rent a botnet to launch DDoS attack on his competitor's website from which the

botmaster can make thousands of dollars per day and the entrepreneur may get indirect benefits by harming the competitor. DDOS has been launched on Spamhaus[9] in retaliation for its decision to add Cyberbunker to its block list. A study by Kaspersky Labs estimated that in 2008, botnet owners earned about twenty million dollars just from launching DDoS attacks.[5][8]

B. Theft of confidential information

Selling personal information harvested from victims can be lucrative as well. Bundled account information, with each account costing from $5 to $20, can be sold to criminals seeking financial fraud or identity theft. Eurograbber, a variant of zeus, was used to steal 36 million euros from about 30,000 bank accounts by compromising their confidential account details[11]. Botnets can earn $20 per record by identity laundering.[5][8]

C. Spam

Bulk lists of email addresses, collected by botnets, can be sold to spammers for $20 to $100 for a million email addresses. Botnets can provide spamming services as well by sending millions of spam mails per day and charging $40 per 20,000 mails. Lethic and Waledac botnets sends about 1.5 - 2 billion spam messages daily. Grum botnet (largest of its time) was used to send billions of pharmaceutical spam mails.[5][8]

D. Pay-per-Click fraud

A botmaster can set up a website inviting the advertisers. Once put, he can use his bots to click on ads. Chameleon,a botnet, generates more than $6 million a month through bogus clicks on online advertisements. Click Forensics estimates that about 17% of ad clicks are fraudulent, approximately one-third of which are directly attributed to botnets netting bot owners tens of millions of dollars annually.[5][8]

E. Bitcoin Mining

By installing bitcoin software on a victim's PC, a bot master can harness the processing power of that computer to mine coins and sell them on the grey or black market for real currency. ZeroAccess botnet generates millions of dollars per year in bitcoin mining. [5][8]

F. Cost of Setting up a botnet

The costs involved are time and efforts to write a sophisticated piece of malware, sustaining and making it undetectable, updating its functionality and maintaining its command and control(C&C) server along with the risk of attribution. But, the value chain of malware that is developed and the risk of prosecution do not grow linearly in terms of cost. For example, a laptop($199.99), a wireless connection(free public wifi), ZeuS builder($7000) or a DIY freeware and anonymous proxy service($102.96) are required to build a cybercrime kit costing $300 to $7302.95 but resulting in profits even in millions of dollars.[12]

Today, getting a botnet up and running costs next to nothing. The leaked Zeus source code is available online for free and a complete Zeus installation for those not very technically skilled for $250. Professional botnet services can cost thousands of dollars per month. Consulting services to assist in setting up a botnet range from $350-$400. Once built, the botnet software will need to be distributed for which Pay per Install (PPI) networks exist to infect computers online and create a botnet from the ground up. Typical PPI networks charge around $100 per 1000 installations. Thus, the profit from the botnet activities dominates the invariably low cost of maintaining a botnet and the ever diminishing degree of knowledge required to manage them[5].

In addition to attacks launched using botnets, there are some other cyber crimes like ransom ware, copyright infringement, cyber espionage, social engineering attacks which can be used for financial benefits or for adversely affecting the economy. Moreover, there is a huge underground market for 'zero day exploits' where hackers sell unpatched vulnerabilities to the first bidder rather than the highest paying bidder, because of the possibility that same vulnerability is discovered, patched and published before they can make profit out of it. Different factors govern the market price of vulnerabilities. If it is patched and published then market price falls to zero. If the security impact caused by this breach is higher, the market price to sell it will also be higher. If the product is very popular, used by many users and difficult to crack, the market price will be higher[10]. For instance, iOS zero day exploit is sold for $100,000-$250,000 while windows exploit costs around $60,000-$120,000[14]. Thus, cyber economics is as important for a professional cyber criminal as for a software vendor or end user. The profit for a cyber criminal also implies loss for some other players in the ecosystem.[13]

CONCLUSION

In this paper, we explored cyber security economics from both the adversary and security vendor's perspectives, and examined the rationale behind their decisions. Cyber adversaries are typically motivated by monetary gains. On the other hand, security vendors are concerned about their own internal goals which may range from upholding the company's image to cost savings on a long term basis. The ecosystem involving these parties is signified by the ongoing process between the two in coming up with schemes to tilt the balance in their favour. Security vendors

deter cyber-attacks by making it unprofitable for adversaries to obtain the desired resource.

It is notable to mention that the current research work does not take into consideration the impact of the clash between cyber adversaries and security vendors on another entity within the ecosystem - the consumers. As users of the products rolled out by security vendors, they stand to lose out from this exchange. Ultimately, companies do not make economic decisions from a user-centric approach. Rather, they would opt to invest in security only for areas which they deem beneficial to them from a financial perspective. Consumers receive benefits only as a by-product of an organisation's internal goals, while bearing the consequences of a company's unwillingness to invest in other areas not aligned with their objectives. This presents an excellent opportunity for adversaries to take advantage of the situation.

Under such circumstances, it would only be fair to hold the security vendors responsible for any potential lapses resultant from their decisions. Punitive measures may be required in forcing security vendors to rethink their security strategies from a user-oriented perspective. While such measures may seem extreme in nature, this would help provide an added boost to the security of the user's machines. This eventually results in the shifting of the balance of the ecosystem away from the adversary's favour and securing a victory for the consumers as a whole.

REFERENCES

[1] Michel Eeten, Johannes Bauer. "ECONOMICS OF MALWARE: SECURITY DECISIONS, INCENTIVES AND EXTERNALITIES". STI WORKING PAPER 2008/Information and Communication Technologies. 29-May-2008.

[2] Tyler Moore. Introducing the Economics of Cybersecurity: Principles and Policy Options. Harvard University.

[3] Ross Anderson and Tyler Moore. Information Security Economics – and Beyond. University of Cambridge. 2006.

[4] N. Kshetri. The Simple Economics of Cybercrimes. IEEE Security and Privacy, Vol. 4, No. 1. January/February 2006.

[5] White Paper : Anatomy of a Botnet. Fortinet. 2013.

[6] Bill Gates. Trustworthy Computing. Email to all full-time employees at Microsoft. January 15, 2002.

[7] Security Development Lifecycle - Benefits of the SDL. Last Accessed: 30 November 2013. http://www.microsoft.com/security/sdl/about/benefits.aspx

[8] Y. Namestnikov, The economics of botnets, Kaspersky Labs, July 2009.

[9] Matthew Prince. The DDoS attack that almost broke the Internet. March 27, 2013. http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet.

[10] B. Prince. Inside the Botnet Business: Getting Rich Quick off Security Threats. August 4, 2010. http://www.eweek.com/c/a/Security/Inside-the-Botnet-Business-Getting-Rich-Quick-off-Security-Threats-597801/.

[11] Steven Musil. Zeus botnet steals $47M from European bank customers. December 5, 2012. http://news.cnet.com/8301-1009_3-57557434-83/zeus-botnet-steals-$47m-from-european-bank-customers/.

[12] Will Gragido, Daniel J Molina, John Pirc and Nick Selby. Blackhatonomics. Publication Date: December 19, 2012 | ISBN-10: 1597497401 | ISBN-13: 978-1597497404 | Edition: 1.

[13] Stefan Frei, Dominik Schatzmann, Bernhard Plattner, Brian Trammel. "Modelling the Security Ecosystem- The Dynamics of (In)Security". The Eighth workshop on the Economics of Information Security(WEIS 2009). 24 June 2009.

[14] A. Greenberg. Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits. March 23, 2012. http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.