Internet Security And The Tragedy Of The Commons

Chris Rose (E-mail: crose@mail.barry.edu), Barry University
Jean Gordon (E-mail: jgordon@mail.barry.edu), Barry University

Abstract

The size, complexity and growth of the Internet have caused numerous security problems for the average user because of the seemingly insurmountable task of securing their computers. Internet security has traditionally been thought of as requiring formal security solutions such as cryptography, firewalls and prescribed security models, but in fact most Internet security problems continue to be caused by users of the system who have no incentive to modify their behavior. Internet security is a shared resource and as such it is affected by the "tragedy of the commons" whereby inactions by some users cause their computers to consume more Internet resources and this causes further deterioration of the network. For example, why should the rest of the Internet continue to suffer because some users have yet to patch their computers from the Code Red worm of many years ago? We propose that the cost of Internet security should be the responsibility of the individual users and a sum of money should be held in deposit for every user of the Internet before they are allowed to join the network and this should be forfeited if inaction from these users then cause network degradation.

1. Introduction

The Internet, the world's largest network, is a public, mutual and self-sustaining network that is accessed by hundreds of millions of people worldwide. It physically uses some the total resources of existing public telecommunications networks but what differentiates the Internet is a common set of the TCP/IP protocols. The Internet has become so embedded into modern life that for many users, for example, the use of electronic mail on the Internet has practically replaced the regular postal service. As the Internet has grown, it has also become the major means for attacking computer systems therefore the growing importance of the Internet and network security issues has caused a shift of security concerns from operating system security to the security of the networks themselves (Kemmerer, 1998).

It is almost impossible for the Internet, or any networked information system to be constructed to successfully prevent attacks and in fact, the natural escalation of offensive threats by hackers countered by defensive countermeasures by system owners has shown that it is virtually impossible to construct a practical system that is invulnerable to attack. Just about every system constructed has been attacked and even presumably sophisticated systems, such as the US Department of Defense, have also shown that it also is susceptible (Smith, Yurcik & Doss, 2001). The Computer Emergency Response Team (CERT) of Carnegie Mellon University has reported 182,463 incidents between 1988 and 2002 and 9,162 vulnerabilities between 1995 and 2002. It is important to note that an incident may involve one site or thousands of sites and that some incidents may involve ongoing activity for long periods of time (CERT, 2003). In fact, the number of security events detected by companies in the first quarter of 2003 jumped nearly 84 percent over the preceding three months (Lemos, 2003).

2. Network Externalities and Computer Security

A network externality arises from the concept that some goods and services are more valuable when more people consume or utilize that good or service and yet these goods and services have little or no value if they are used without a network (Katz & Shapiro, 1995). Typical examples of these would be telephones and fax machines as people who own these products would form a network so as to be able to exchange information and provide a way for people to communicate with each other. The more people who have telephones the more valuable this network becomes. Electronic networks such as communication and information networks are said to exhibit positive production and consumption externalities since the value of the good that is a part of the network increases with the number of units sold since each unit complements each other that in turn will increase the value of the component.

In security it can also be said that an externality is when one person's actions has an effect on others, such as when LoJack is introduced in a city then the theft of cars goes down, since thieves cannot tell if LoJack is installed or not. The attributes of computer security suggests that computer security is an externality, since the lack of security on one machine can adversely affect the security on many other machines, such as when credit card numbers are stolen from an improperly secured machine and are used to commit crimes at other web sites. Because computer security is an externality the prices of hardware or software neither reflects the possibilities of security failures or the damage associated with them (Camp & Wolfram, 2000).

3. The Tragedy of the Commons

William Forster Lloyd, an amateur nineteenth century mathematician, wrote a seminal treatise on the deterioration that would occur in a pasture due to the innate traits of humans. This became known as the "tragedy of the commons" and it was resurrected into mainstream academia by a biologist, Garrett Hardin in 1968. Although Lloyd was examining a shared pasture, his principles can be extended to most shared resources including the Internet. Basically, if a resource is used at a rate that is near capacity then additional users will only deteriorate the value to all users. This leads to a vicious cycle whereby all users attempt to consume more of the resource so as to be in the same position as they were before the additional user started consuming the resource. Each user is in fact pursuing their own best interest but this ultimately just causes the demise of the resource (Turner, 1993).

Some authors have postulated that the Internet is not really a commons and, for example, Quarterman (1997) gave reasons for that position:

- The resources of the Internet are inexhaustible
- If some parts of the Internet were to be immediately saturated, a few moments later all that bandwidth would be available for use
- Passing data through an IP link doesn't produce the kind of wear that happens when a machine is used or a plant is consumed
- Using the Internet makes it grow since every new user pays money to an ISP which uses that money to purchase additional equipment.

These arguments may make some rational sense in the traditional sense of the everyday use of the Internet but this does not take into account the problems of Internet security. Distributed Denial of Service (DDoS) attacks occur when a number of machines with vulnerabilities are taken over and controlled by hackers and used to flood a specific machine with worthless packets of data. These have become a serious problem since 1999 and they are at the heart of "the tragedy of the commons" since while everyone might be interested in protecting the shared resource of Internet security, the individual had a stronger incentive to cheat by connecting insecure computers (Yan, Early and Anderson (2000).

4. Security

Current approaches to security of information systems to prevent attacks have traditionally been thought of as requiring increased defenses by using the formal methods of encryption, authentication and layered network devices, such as firewalls and network intrusion detection systems. Security in hardware and particularly in software is today done by the penetrate-and-patch approach whereby when someone finds vulnerabilities in a system, or what is called an exploitable security hole, then the manufacturer issues a patch to correct the vulnerability. The problem is also compounded by the fact that there are executable attack scripts that can be anonymously downloaded from various sites and additionally, most of the computers in the world operate with some sort of Microsoft software which makes it possible that a single vulnerability will have wide-ranging and devastating effects (Smith, Yurcik & Doss, 2001).

An individual can do very little to stop a Distributed Denial of Service (DDoS) attack since this type of attack exploits the vulnerabilities of other computers on the network and while someone might be willing to pay $100 to prevent themselves from being attacked, it is much less likely that they will spend that sum to stop Microsoft or Amazon from being attacked, since it might be more rational for that user to keep that $100 in their pocket and hope that they are not one of the small minority that becomes a target (Yan, Early and Anderson (2000).

Although DDoS attacks may make the headlines, most Internet security problems are caused by worms and viruses and many of these are old and easily preventable. Lemos (2002) stated that 9 months after the Code Red worm first appeared, more than 18,000 systems appear to still be infected and with a simple command, all the machines could be co-opted into an attack that could take down any Web site. He also stated that a network security company that had established a monitoring system still received nearly 30 probes by infected Code Red servers every minute. Recently there has also been the emergence of the first flash worm, which is an automated attack program that spreads so quickly that persons who normally react to security vulnerabilities can't react fast enough. The worm, SQL Slammer, infected 200,000 computers running Microsoft's SQL Server software that hadn't had a 6-month-old patch applied. The worm is thought to have spread to 90 percent of all vulnerable servers in the first 10 minutes after it had been released on the Internet. More importantly, online vandals are putting more effort into exploiting existing flaws than finding new ones (Lemos, 2003).

These reports demonstrate that many of the security problems on the Internet are as a result of the inaction by the users to vulnerabilities that have been known for many months. If 200,000 servers running Microsoft software became infected because they did not apply a 6-month old patch and since this inaction by the users affected every other user of the Internet, it can be argued that these users who did not patch their computers are consuming more of the shared resource (the Internet) and are reducing the amount of that resource available to other users which causes a degradation of the shared resource.

5. Economic Liability

It is difficult to define the consequences of a vulnerability especially before they are found but it has been suggested that the consequences of a vulnerability should be defined by the amount of processing power of that machine. However, the bandwidth available to the machine or the information contained in the machine might be more important (Schechter, 2002). Camp and Wolfram (2000) listed two methods of pricing security, either computer owners could be charged for having vulnerabilities or coders could be charged for creating them. However, they suggested a third method which would be that every computer, regardless if it is a client or a server, be allocated certain initial properties and also a set of vulnerability credits similar to those used in industry to deal with pollution.

Varian (2000) stated that one of the fundamental principles of the economic analysis of liability is that it should be assigned to the party that can do the best job of managing risk and although organizations are in a better position to manage risks than are the users, the users should not escape all liability for their actions. If the party that is in a position to protect a system is not the party that would suffer from the results of a failure of security then there will be problems. “While individual computer users might be happy to spend $100 on anti-virus software to protect themselves against attack, they are unlikely to spend even $1 on software to prevent their machine being used to attack a third party such as Amazon or Microsoft” (Anderson, 2001). “One reason that computer security is so poor in practice is that the liability is so diffuse. Consider the attacks that took place a few months ago, in which computer vandals took over computers on relatively unprotected university networks and used them to shut down Yahoo and other major Web sites. Although the universities found the takeover of their machines a nuisance, they didn't bear the bulk of the costs of the attack on Yahoo. But if universities bore some liability for the damages to third parties, they would have a stronger incentive to make their networks more secure" (Varian, 2000).

6. Economic Solution

A major problem with voluntary solutions to the tragedy of the commons is the "free-rider problem" which simply means that an individual will resist paying for a shared resource if they know that other users of the resource will pay for it and they will be able to freely use it (Turner, 1993). Camp and Wolfram (2000) have suggested developing a market for the detection of security failures so that those persons who failed to secure their networks would be facing a formal pricing structure to compensate for these security failures. This market, they suggest, should include both commercial users and home users since if home users were not a part of this market then the overall ability of the market to respond to security would suffer.

One of the only means for averting the tragedy of the commons is to mutually agree on mutual coercion in which either freedom is traded for the greater good of the system or some sort of penalty is imposed for overusing the resource. The users of the resource have to realize that the survival of the system requires short-term sacrifices in return for long-term gains and the users should have enough knowledge to know that there are long-term dangers and gains due to the common resource. Therefore the designers of the system should make sure that there are shared common goals of preserving the commons and that these have priority over individual goals or the commons are in jeopardy (Turner, 1993). It has been suggested that if the government introduces economic penalties to individual users who fail to secure their personal computing devices then this would be thought to be an excessive intrusion and therefore politically infeasible (Schechter, 2002).

However, we argue that in all modern societies, deposits on publicly available resources are the norm and in fact very few users of these resources object to paying the provider a security deposit for telephone, electricity or water and these deposits are forfeited in the event of abuse of the system. For example, Bellsouth, a large regional provider of telephone services, usually requires a deposit and as an example, their Long Distance Service Agreement for Residential Customers states that one of the reasons for requiring a deposit is if there has been "fraudulent, illegal or abusive use of any BellSouth Long Distance services during the previous five years, then we may require that you place a deposit with us or make an advance payment to secure payment for the Services we provide to you. If you refuse to make a deposit or advance payment, we reserve the right to refuse to provide you Service" (BellSouth, 2003).

It can reasonably be argued that if other publicly available resources require a deposit and that this deposit is forfeited whenever there is abuse of the system, then a deposit should also be required from the users of the Internet. This deposit should be paid to the Internet Service Provided (ISP) whenever someone joins the network to use the Internet and we argue that this deposit should be based on both the processing power of the machine and the bandwidth available to it. We further believe that this deposit should be forfeited whenever the user of the system fails to apply a patch to a known vulnerability.

There are some problems with this solution however, and chief of these is a method to reliably ensure that the users of the network are notified in a timely and reliable manner whenever a patch for a vulnerability is released. However, most modern software, including those from Microsoft (which are the source of most vulnerabilities), have an option to automatically search for updates, but many users do not use this feature perhaps because of a fear that this feature will pass private information on to the manufacturer. Secondly, there is the problem of the timeframe that should be allowed to the user to update their machines but we believe that this should be measured in days and not weeks or months. There is also the question of who should be the beneficiary of these forfeited deposits but it can logically be argued that the main entity entrusted with security on the Internet, CERT, should be the recipient.

Conclusion

Most Internet security problems are caused by users of the network who have no incentive to apply the necessary remedial action to their computer which in turn causes these computers to be vulnerable to known exploits. These patches are provided by the manufacturers and are available to all users of the affected software/hardware but inaction on the part of these users cause their computers to be vulnerable and when attacked, these computers now begin to consume more of the shared resource (the Internet) thereby degrading the service which affects the other users of the resource.

We propose that every user of the Internet be charged a deposit, similar to a deposit payable on many other public resources, and that this deposit be forfeited by the user if they fail to take action whenever a vulnerability is announced. However, further research has to be undertaken to identify and streamline the method of notification used by the manufacturers of the hardware/software so that all users of their products are instantly notified whenever a patch is released. If these users are not coerced into applying the necessary remedial action then their inaction leads to the growing problem of Internet security and the tragedy of the commons. 🕮

References

1. Anderson, R. (2001, January 30). "Why information security is hard – an economic perspective", Proceedings of the 17th Annual Computer Security Applications Conference.
2. Bellsouth (2003) "Long Distance Service Agreement for Residential Customers", Retrieved from the World Wide Web on 4/2/03 from *http://www.bellsouth.com/bsldcc/at_home/pdfs/serv_agreement_residential.pdf*.
3. Camp, L. and Wolfram, C. (2000, October 24). "Pricing security", Proceedings of the CERT Information Survivability Workshop, Boston, MA.
4. "Computer Emergency Response Team (CERT)", Retrieved from the World Wide Web on February 28, 2003 from *http://www.cert.org/stats/#incidents*.
5. Dingledine, R. and Syverson P. (2002). "Open issues in the economics of anonymity", *The Free Haven Project*.
6. Katz, M. and Shapiro, C. (1995, June) "Network Externalities, Competition and Compatibility", *American Economic Review*.
7. Kemmerer, R. (1998) *Secure Computing on the Internet*. Computer Science Department, University of California.
8. Leiwo, J. and Heikkuri, S. (1998). *An analysis of ethics as a foundation of information security in distributed systems*. 31st Hawaiian International Conference on System Sciences.
9. Lemos, R. (2002, May 3) "Code Red still threatens net", *C-net News*. Retrieved from the World Wide Web on 4/4/03 from *http://news.com.com/2100-1001-899245.html*.
10. Lemos, R. (2003, April 3) "Worms boost cyberattack stats for 2003", *C-net News*. Retrieved from the World Wide Web on 4/4/03 from *http://news.com.com/2100-1009-995380.html?tag=lh*.
11. Odlyzko, A. (1999, July 26). "The visible problems of the invisible computer", *First Monday*, vol. 4, no. 9.
12. Quarterman, J. (1997, November) "Is the Internet a Commons?", *Media Matrix News*. Retrieved from the World Wide Web on 3/30/03 from *http://www.mids.org/mn/711/commons.html*.
13. Ramakrishnan, C. and Sekar R. (1998) "Model-based vulnerability of computer systems", *2nd International Workshop on Verification, Model Checking and Abstract Interpretation*.
14. Schechter, S. (2002, May 17). *Quantitatively differentiating system security*. Harvard University.
15. Turner, R. (1993, January 21). "The tragedy of the commons and distributed AI systems", *Proceedings of the 12th. International Workshop on Distributed Artificial Intelligence*, Hidden Valley, PA.
16. Smith, B., Yurcik, W., and Doss, D. (2001, October 18) "Ethical hacking: the security justification", *Proceedings of the Ethics of Electronic Information in the 21st Century Symposium*.
17. Varian, H. (2000, June 1). "Managing online security risks", *Economic Science Column, The New York Times*. Retrieved from the World Wide Web on March 25, 2003 from *http://www.nytimes.com/library/financial/columns/060100econ-scene.html*.

18. Yahalom, R. (2002, May 8) “Liability transfers in network exchanges”, *Workshop on Economics and Information Security*, University of California, Berkeley 2002.
19. Yan, J., Early, S. and Anderson, R. (2000) “The XenoService – A Distributed Defeat for Distributed Denial of Service”, *Proceedings of Information Survivability Workshop*, Boston, Massachusetts, USA.
20. Yurcik, W., Doss, D. and Kruse, H. (2000) *Survivability-over-security: providing whole system assurance*, Illinois State University.

Notes