Author(s): Hossein Jahankhani, Branko Antonijevic, Terry Walcott
Article Title: Evaluation of tools for protection of interest against hacking and cracking
Year of publication: 2008
Citation: Jahankhani, H., Antonijevic, B., Walcott, T. (2008) 'Evaluation of tools for protection of interest against hacking and cracking', *Communications in Computer and Information Science*, 12(1), pp.54-58

Link to published version:
DOI: 10.1007/978-3-540-69403-8_7

Evaluation of tools for protection of interest against hacking and cracking

Hossein Jahankani, Branko Antonijevic, Terry Walcott
University of East London
h.jahankhani@uel.ac.uk

Abstract : The internet considered a tool that effectively ensures communication globally has been hindered by hackers and crackers continuously. In so doing, a multitude of network facilitated tools such as firewalls, virtual private networks (VPN) and a variety of antivirus software packages has been enabled for dealing with such predicaments. However, more often than not these facilitated tools are marketed as perfect solutions to the ever culminating problems such as loss of data and privacy in networked and world wide intercommunications. We provide a forum for addressing these perceived problems in this paper.

Keywords: Firewall, Hacker, Network security, vulnerability analysis

1 Introduction

Firewall and other security software have got the power to control the flow and access to information available to user at any given moment. It is therefore used by the governments and internet providers to determine what we are allowed to view on the net or used for business orientated means to protect the access to system or data on private networks. It is a very delicate position of power. Are the major players like government, consumers, Non Government Organisations (NGO), hackers, major software companies, all striving for the common goal or are they deliberately making the whole situation confusing for various reasons? The aim is to transparently evaluate tools for protection of interest against hacking and cracking and show the hidden interests of all parties involved by using data matching techniques to contrast their statements and present them in a balanced view. Combination of pressure on the companies to reduce expenses, freely available hacking tools, fewer plans to increase security due to the issue being downgraded in importance (Jahankhani et al, 2007) is causing new threats to the network security.

Protection against Hacking and Cracking

There are many associated bodies that determine the likelihood of protection software being useful to protect core business processes. We present here stakeholders such as the government, consumers, non-governmental organisations (NGO) and major software companies such as McAfee.

Government

Government is laying down the standards and regulations by which software companies need to comply. This is to insure a safe and manageable environment in which competitors, can compete and operate by the same set of rules and standards. The main focus is on the standard industry issues as an older generation, which mainly makes the government, uncomfortable and confusing in an unfamiliar territory of this fast moving environment faced with sudden changes. According to Richard Allan– Cisco (Allan, 2006), it is only when it becomes a newspaper big story that the parliament act and it takes good few years for the wheel to spin.

NGO

An example of NGO in IT is British Computing Society, which is looking after IT professionals in industry. It is financially independent from industry and government funds so it is building its position through close working relationship with all parties with an agenda of improving recognition for IT professionals. Others are ISCA Labs and West Coat Labs which are certifying firewalls with aim to bring industry recognised standards (Harris and Hunt, 1999).

Consumers

Consumers are represented by different UK regulators like Ofcom, Financial Services Authority, Ofgem which, although set up by the government, are acting independently in the interest of consumers.

Hackers

Hackers are IT professionals writing some very intelligent programmes and indulging themselves in problems solving sessions. It is very important that we do not confuse them with crackers whose only interest lies in breaking in security system for malicious purposes (Jahankhani et al, 2007).

Leading security software companies

Leading security software companies are Cisco, Check Point, Fortinet, Symantec and McAfee. Open source firewall are also available most companies are playing safe by using major commercial products (Potter, 2006).

Real and perceived threats to our networks

Cisco's Pix, Checkpoint's Firewall-1 and FortiNet's FortiGate are the front runners in regards to securing perceived threats. Personal users are more limited to popular software provided by Symantec or McAfee. They are all marketed as the end of all problems by being absolutely secure. Hackers have shown in presentations such as the "Black Hat" presentation (Hancock, 2000) that even Firewall-1 is easily penetrated. The problems with firewall can be in its design, implementation or configuration, and huge log of data which need to be managed by highly skilled staff. The set of rules are static and another approach is to make these rules flexible or interactive so that they adapt instantly to different types of attacks.

Many of the firewalls can be strengthened by employing simple procedures such as better staff training, simplifying monitoring roles by disabling all unnecessary functionalities on the network. In addition this can be enhanced by looking at the way a firewall is implemented and by checking its configuration for any abnormalities done by faulty or unauthorised configurations.

According to reports undertaken by Frost & Sullivan (2001), smaller companies feel they are lacking the funds to implement firewalls because its cost effectiveness cannot be justified. For this reason, major software distributors are educating smaller firms in order to demonstrate the impact that an ineffective firewall infrastructure can have on such types of firms. This has led to a 47.67% increase in firewall markets from 2000 to 2001 and the revenue was predicted to grow from $604.1 millions in 2001 to $1,249.3 millions by 2005 with average growth of 31.78% a year as stipulated in fig.1. That was the reason for scaling the firewalls down, to educate us the end users, as even our home systems are under a threat. However, there is a greater need for securing our networks for both the consumer and governmental bodies. This in effect should delimit marketing only geared towards imposing panic buying. In other words, this type of marketing will encourage the purchasing of products that are not delivering on the promises to safeguard our information systems.

Total Firewall Market: Revenue Forecasts (Europe), 1998-2005

Year	Revenues ($ Millions) Software	Revenues ($ Millions) Appliances	Revenues ($ Millions) Total	Total Revenue Growth Rate (%)
1998	78.3	59.1	137.4	---
1999	112.7	98.6	211.3	53.78
2000	189.3	219.8	409.1	93.61
2001	266.7	337.4	604.1	47.67
2002	337.5	460.1	797.6	32.03
2003	377.6	573.1	950.7	19.20
2004	433.3	668.9	1102.2	15.93
2005	478.2	771.1	1249.3	13.35
CAGR(1998-2005)	37.86%	17.98%	15.64%	---
CAGR (2001-2005)	25.38%	12.39%	31.78%	---

Note: All figures are rounded. Source: Frost & Sullivan

Figure1. Total Firewall Market: Revenues Forecasts (Europe), 1998-2005

Criminalising hacking tools

The Fraud Act 2006 is tackling the fraud by false representation which is used in spoofing and phishing which is used in internet related crime. Many administrator tools have a dual use. The program may be developed for a genuinely good purpose and because of its functionalities often ends up on a hacker web site as an available hacking tool. Security Administrator Tool for Analysing Networks (SATAN) is one examples developed by Dan Farmer and Wietze Venema in 1995, it was designed to be an automated testing software looking for weaknesses in the system and was an instant hit with hackers. Such issues need to be discussed and clarified further so that academics, developers and other interested parties who are developing useful diagnostic tools do not end up being prosecuted (Sommer, 2006).

Guillaume Tena, a security researcher, was fined 6000 euros and got a suspended jail sentence, based on a claim of copyright infringement,(Dudley-Goug, 2005) for publishing his findings that a software that claimed to be able 100% had flaws.

Staff Training and enforcement of the security policies

One of the most important tools against hacking and cracking are staff and consequently first stage in building a spoof web site is in collecting a correct data about the site involved. Helpful secretaries are too happy to give away important data on key members of staff without necessary precautions thus, making the social engineering top five tools for hacking into a system. The same can be easily applied to guessed passwords on important accounts; default password on Network Protocols; lack of updating operating systems and simply loosing companies laptop which has an access to a whole company's network (Wood, 2006). Remedies are fairly simple. The company's internal policy should clearly state who should give information on staff and procedure on password change should be followed at all times.

Conclusion

Firewall is no longer used as the ultimate security system and it is increasingly being incorporated into a more multilayer, cascading, cross-referencing systems (Smith et al, 2003). Dilemma which is often based on how much to invest in the security system is now more clarified. Companies are investing in stages rather than 'all at once' so that at any given moment in time their software is not completely outdated but only small segment of the system needs to be updated from time to time. In that way the firewall grows in the integrated security system.

Staff in the company can be tricked into giving away sensitive information like passwords, access to the whole or parts of the system. Small information from different parties can be used to get new information using data matching process in order to gain access to unauthorised segments of

the system. Staff training is highly recommended as less expensive way to improve our security defence. It is actually a vital peace of the puzzle as no matter how effective and certified it is for good quality the firewall and other security software will not perform as projected unless properly implemented. Another area in which training help us save money is proper configurations and product update for any shortcomings that appear in the teething process of system implementation. The staff training will also give us an insight into broader aspects of security and help us choose future firewall to suit our needs on any related product. Choosing the right product, being fully informed, is helping integrate our systems quicker and safer as there will be less conflicting problems in the system that need to be resolved thus making the system simpler in its architectural structure.

No security software will be 100% fool proof as it is vulnerable to technological innovation and changes which open other unexplored and unexpected alleyways. It will always be a race between making a new, more advanced technologies and exploiting its new vulnerabilities before they are spotted and rectified.

According to He (2006), internet routing protocols should be intrusion tolerant by maintaining its operations while under attack, identifying malfunctions in router and immediately isolating such anomalies in the protocol. The future lies in making security systems being as simple as possible with interactive artificial Intelligence such fully integrated decision-making instrument that will be able to provide data matching, fingerprinting, biometric checking for identifying objects in the system regardless of it being human or a machine enabled system.

References

Allan, R. (2006). 'Politics of Internet Security', University of Cambridge Computer, Laboratory, Accessed: 21.11.2006.

Dudley-Gough,N.(2005). 'Jail for bug finding researcher?', *Network Security*,pp. 1- 20.

Hancock, B.(2000). 'Hackers Breach Firewall-1", *Computers and Security*,19(6),pp. 496- 497.

Harris,B and Hunt,R.(1999). 'Firewall Certification', *Computers and Security*, 18(2), pp. 65-177.

He,L.(2006).'Recent developments in securing Internet routing protocols',BT Technology Journal,24(4), pp. 180-196.

Jahankani,H., Shanta,F., Nkhoma,M.Z., Mourtadis,H.(2007).'InformationSystem Security', *International Journal of Information Security and Privacy*, 3,pp. 13-25.

McGraw,G.(2002). 'Building secure software: better than protecting bad software', *IEEE Software*, 19(6), pp. 57-58.

Potter,B. (2006). 'Open source firewall alternatives', *Network Security*, 1,pp.16-17.

Smith,R.N., Chen,Y., and Bhattacharya,S.(2003). 'Cascade of Distributed and Cooperating Firewalls in a Secure Data Network', *IEEE Transactions on Knowledge and Data Engineering*, 15(5*), pp. 1307-1315*.

Sommer, P. (2006). 'Criminalising Hacking Tools', *Digital Investigation, 3, pp.68-72.*

Wood,P,(2006). 'The hacker's top five routes into the network (and how to block them)', *Network Security*,2,
pp. 5-9.

Xin, L.(2007). 'Defeating Active Phishing Attacks for Web-Based Transactions', *International Journal of Information Security and Privacy*,3, pp. 47-60.