Effective Approach Toward Intrusion Detection and Pretention Systems in Implementing Defense in Depth

Basant Kumar
Computer Science, MCBS,Muscat,
Sultanate of Oman

***Abstract*—Recently hackers have compromised and broken into number of the most secure networks in the world causing loss of sensitive data, breach of privacy, compromising confidentiality and raising threats to national and international community. This devastating situation has led security experts to question the effectiveness and reliability of current security systems against hacking attacks.**

It is indeed a fact an intrusion detection is the action of trailing activities in a network or a computer system to identify a threat that disrupts policies of information security, whereas intrusion thwarts the malicious activity from attacking the systems. The main obstacles are being unable to observe and keep track of the widely used systems and also having a problem in responding promptly in case if there is any attack getting triggered. This paper describes defense in depth with an integration of several security tools applied using an onion model on its various layers as a unified security system.

Keywords*— *Attacks; intrusion detection system; threat matrix; defense in depth; unified security system

I. INTRODUCTION

Hacking relates to many fields starting from risks and challenges that face the provision of information services, to a detailed number of interwoven subject areas that need to be addressed directly because of its criticality to operations, reputation, and economic stability. However, despite hackers' threats, enterprises have to stay connected with the internet for successful competition in today business world, as hackers are finding new methods to bypass protection systems and mount very effective internet-borne hacking attacks [1].

To analyze hackers activities and as mentioned by [2] [3] state that the success of security programs depends upon the capability in analyzing behavior and detection of hacking processes that information systems are subject to, through various ways, including firstly, human error related, such as direct download from untrusted websites and unreliable sources, unawareness of e-mail attachments, and sharing files and portable devices. Secondly, potential hackers' man-in-the middle attacks techniques such as technical interception using eavesdropping and packet sniffing. Then attacking major information system components and security devices via reconnaissance and applying ARP poisoning, URL flooding, IP spoofing and port redirections. In addition, web scripting and brute force attacks, and identity thefts. And finally, one of the hacking ways is the plantation of viruses, worms and Trojan horses and dissemination via zombies, an example is backdoors, spyware and man-in-browser attacks and last hacking stage is denial of service.

Conforming to these hacking activities [11]has broken hacking into nine processes, Footprinting, Scanning and Enumeration, Gaining access, Escalating of privileges, Pilfering, Covering tracks, placing backdoors, and finally Denial of service. Table I compares these hacking processes from [4] to other hacking techniques from [5][6][7] .

Table I: The Hacking Processes

	McClure, S. Scambray, J. Kurtz G. *Hacking Exposed Network Security Secrets and Solutions*. 7th edition. McGraw-Hill/ Osborne (USA). 2012	Harold F. Tipton and Micki Krause. *Information Security Management Handbook. 6th Edition*. Auerbach Publication (USA). 2007	Christian Barnes, Tony Bautts, Donald Lloyd, Cric Ouellet, Jeffrey Postuns, David M. Zudzian and Neal O'Farrel. *Hack Proofing Your Wireless Network*. Syngress (USA). 2002	Robert Schifreen. *Defeating the Hackers*. Wiley (UK). 2006
	[4]	[7]	[6]	[5]
Footprinting	√	Physical access	Conducting reconnaissance	Search engines, social Engineering
Scanning	√	Network mapping and port scanning, vulnerability scanning, sniffing	Sniffing,interception and eaves-dropping	Data interception, provisioning and identity management
Enumeration	√	Network exploits. spoofing, fingerprinting, wardialing/wireless war driving	Network hijacking and modification, spoofing	
Gaining Access	√	Stack based buffer overflow, cross site scripting,	Unauthorized access	E-commerce fraud

		password cracking, session hijacking		
Escalating Privileges	√	Trojan horses and rootkits	Stealing user devices	Data theft
Pilfering	√			
Covering Tracks	√		Introduction of malware	
Creating Backdoors	√	√		
DOS	√	√	√	√

II. PROBLEM STATEMENT

There has been a predicament when it comes to the protection of the flows of information and data. People have come up with various methods of protecting and safely transferring information. Technology has become more advanced, communications and information systems are developing, and the information security issues have become more complex. This problem has been accelerated by the extensive use of the internet, wireless and wired communications, and web applications. Firms depend entirely on them but unfortunately, they are vulnerable to serious security challenges, which creates the obligation of implementing methods that can identify the problems and protect computer systems against them. Such methods include authentication, firewalls, intrusion detection systems (IDS), and encryption.
The main obstacles are being unable to observe and keep track of the widely used systems and having a problem in responding promptly in case if there is any attacks getting triggered. The paper proclaims and analyze different threats pertaining to the outcomes from threat matrix and techniques of intrusions detection.

Despite the great advances and researches in defense-in-depth techniques, information systems are still encounter a massive growing in the security breaches which are always taking the lead as hackers are always ahead in discovering system vulnerabilities that open doors for all kinds of hacking attacks conforming to these hacking activities which are broken into several processes such as

- Footprinting and Reconnaissance
- Port Scanning and Network scanning
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing and spoofing
- Social Engineering
- Denial-of-Service and DDOS
- DNS poisoning and Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection attack
- Hacking Wireless Networks
- Hacking Mobile Platforms

III. METHODOLOGY

Risk evaluation and threat modeling occurs in three steps which are:

Evaluation of risk: Identify amount of the loss.

1- Identify prospective threats : determine the several things your program code does that could possibly be attacked (as well as things that libraries and frameworks do as your representative)
2- Threats Mitigation: make sure that parts of your program code that could possibly be attacked are properly secured.

A. Generic Threat Matrix (GMT)

The threat matrix as shown in Table II is arranged into several levels of magnitude, where every level is corresponding to distinct sort of threat [8][9].

Table II: Threat Matrix

Threat Matrix									
Vulnerabilities / Threats	O.S	Application	Network	Firewall	Insecure Wireless	Server	Hardware	Database	Total Score
DOS	✓		✓			✓			3
DDOS	✓	✓	✓	✓		✓			5
SQL Injection		✓						✓	2
Password Attack	✓	✓	✓	✓	✓			✓	5
Cross Site Srcipting (XSS)		✓							1
Phishing		✓							1
Buffer over flow		✓					✓		2
Session Hijacking		✓				✓			2
IP Spoofing			✓	✓					2
Sniffing		✓			✓				2
Man in the Middle			✓	✓				✓	3
Port Scanning			✓						1
Malware threats	✓	✓	✓	✓	✓	✓		✓	7
Total Score	4	9	7	5	3	4	1	4	36

Table II clearly addresses different type of security threats and vulnerabilities that attackers can use to access and exploit vulnerable systems, application and networks.

B. Attack Vectors

Attack Vector is a mechanism or method used by the attackers to access target network, victim machine or system for the intent of conducting an attack, information gathering, injecting malware, etc. For the attack vectors, particular vectors used particular, related attack metrics [10] .Various attack vectors are as following:

- Phishing Attacks
- DOS
- DDOS
- Password attack (Unsafe)
- SQL Injection (Database)

Others:

- Unsecured Wireless Networks
- Removable Media
- Malicious Web Components (XSS)
- Viruses and Malware (Ransomware)
- Protocol vulnerability
- Vulnerable port
- Software bugs

C. Risk Assessment

Fig. 1. shows the rate of threats per an asset or vulnerabilities. The highest score of threats that can be found with the given set of vulnerabilities is the Malware. This type of the risk has impact most of the given assets, which leads to hardware failure, data loss or damaged etc. There are different types of malware attacks, Wannacry ransomware is an example of recently malware attacks that encrypt victims data assets and asking for ransomware for decryption. It spreads globally causes significant loses and affecting both at enterprise and individual levels.

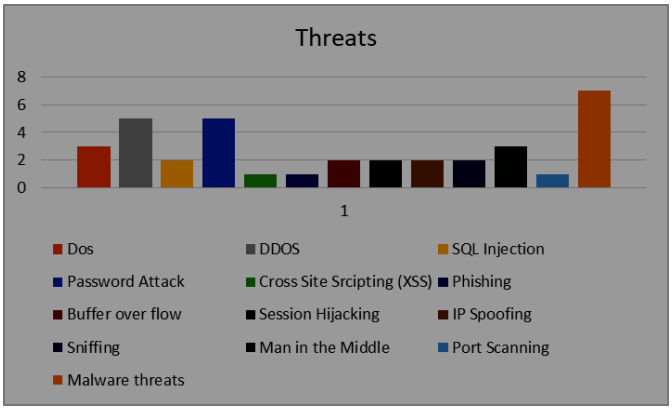

Fig. 1. Total score of threats per asset

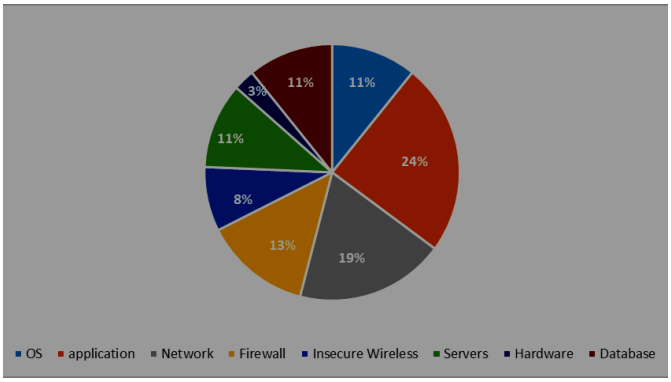

Fig. 2. Mapping threats percentage against vulnerabilities

Fig. 2. illustrates the each asset and rate of threats that can impacting it, where the applications are the most vulnerable asset with approximately of 24% among all. Most of business transactions are now available over the internet through online applications. Many applications could be vulnerable to different type of attacks and exploitation. Maintaining security countermeasures for application and systems are so crucial to protect against intrusions and security breaches. Cybercriminals continues developing methods for hacking systems and application, for example, injecting malicious codes within the application, attracting the users to reveals their login credentials with faking and attractive ways

IV DEFENSE IN DEPTH TECHNIQUES

Enhanced defense-in-depth (DID) is one the major hacking defense components which provides a layered onion type security that is preferred compared to egg-shell approach that is a single strong protection layer. This paper[11] states that "defense-in-depth can be gained by thinking of it as forming the layers of an onion, with data at the core of the onion, people as the outer layer of the onion, and network security, host-based security and application security forming the inner layers of the onion". The onion type approach contains multilayer defense systems, one after another, so, if an intruder breaks into the system through one defense system, he or she faces the second then the third, which makes the defense systems much harder to break with respect to time, knowledge and effort. This paper[12] also presented a defense-in-depth strategy with seven layers of protective measures, in a sense that if one fails the other layer takes over as follows, identifying risks and requirement, network/application firewalls, authentication, configuration, host-based firewall, encryption, and finally awareness and training. In addition, this seven layers defense-in-depth strategy from [12] is also supported by others as in Table III.

Table III Defense-in-Depth Tools and Techniques

	Fadia, A. *The Unofficial Guide to Ethical Hacking*.2nd edition. Thomson Course Technology(Canada).2006	Ali Jahangiri. *Practical hacking and counterm easures*. Ali Jahangiri Org (USA). 2009	Harold F. Tipton and Micki Krause. *Information Security Management Handbook. 6th Edition*. Auerbach Publication (USA). 2007	Sattarova Feruza Y. and Tao-hoon Kim. IT Security Review. Privacy, Protection, Access Control, Assurance and System Security. International Journal of Multimedia and Ubiquitous Engineering. Vol. 2, No. 2. April, 2007. Pages. 17-31	Christopher J. May, Josh Hammerstein, Jeff Mattson and Kristopher Rush. *White Paper. Defense-in-Depth. Foundations for Secure and Resilient IT Enterprises* (CMU/SEI-2006-HB-003). Carnegie Mellon University. September 2006	US-CERT. *White Paper. Recommended Practice. Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies*. U.S. Department of Homeland Security. October 2009
	[29]	[2]	[7]	[11]	[30]	[31]
Information Security Awareness	√	√	√	√	√	√
Malicious Insiders and Anomaly Detection	√	√	√	√	√	√
Access Control	√	√	√	√	√	√
Encryption	√	√	√	√	√	√
Sniffing and Spam Filters	√	√	√	√	√	√
Data Leak Prevention	√	√	√	√	√	√
Secure links	√	√	√	√	√	√
Firewalls	√	√	√	√	√	√
Intrusion Detection and Systems	√	√	√	√	√	√

This paper describes a defense-in-depth strategy with seven layers of protective measures using table III as in a sense that if one fails the other layer takes over as follows, identifying risks and requirement, network/application firewalls, authentication, configuration, host-based firewall, encryption, and finally awareness and training.

V. HIDING AND DECEPTION TECHNIQUE

The simplest hiding techniques is network address translation (NAT), which may be used as a simple hiding tool that gives screening against hackers[13]. In a more specialized way, this paper [14] gives an important countermeasure method against hacking that is to go invisible and hide resources from hackers using deception techniques. Hiding techniques prevents hackers from getting correct or complete information about the hidden assets' attributes or existence. This paper [28] used packets hiding methods for preventing selective jamming attacks. Another technique in hiding is placing servers and files in unexpected locations or names, and/or modify server's banner to show incorrect information such as version and model number. Hiding may be used to hide information security components such as honeypots, intrusion detection systems, key loggers, servers and firewalls. A bogus ICMP message can be disseminated by the firewall to deviate the hacker's sensor to change the flow of information and finally diminish hacker's recognition capability, eventually misdirect and disrupt the identification process of the hacker [14].

However, this paper [15] has suggested a solution that prevents backdoor logic from turning on untrusted hardware component. The principle idea is to scramble inputs that are supplied to the hardware units at runtime, making it impossible for malicious constituents to gain the information they need to execute malicious actions to make the system vulnerable.

There are also two major hiding and deception techniques that are essential, one is hiding information during transition, like obfuscation of the source and destination nodes[16,17,18,19,20,21] and the second is Honeypots that mislead hackers to a fake system[22,23,24,25,26,27].

VI.ENHANCE SECURITY IN WEP

Furthermore, to enhance the highest security level of WEP we must change the default service set identifier (SSID) and passwords for network devices. Although, modifying WEP by utilizing Temporal Key Integrity Protocol (TKIP) will enable a maximum security nevertheless, we can provide cryptographically secure communication and standard encryption algorithm such as AES (Advanced Encryption Standard).CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) utilizes AES in cipher clock chaining mode to produce a MAC and to encrypt the message. Of course, this is the most secure way to transfer confidential information wirelessly. Both CCMP and TKIP are new 802.11i standard.

Enable the highest level of WEP that existing hardware provides. WEP provides some security and is effective in deterring casual attempts by outsiders to infiltrate network. Most 802.11b certified products can use basic 64 bit WEP encryption. By default, however, 64-bit encryption may be disabled.

VII. WPA 2 SECURITY

The most secure and emphatic method to provide cryptographically secure communication is to use well known and studied standard encryption algorithm such as AES,CCMP utilizes AES in cipher-clock-chaining mode to produce a MAC and to encrypt the message. This is certainly the most secure way to transfer confidential information wirelessly.

Access points or wireless routers ship from the manufacturer with default SSID and passwords must be changed as leaving these at default makes it easy for a malicious outsider to gain access.

Modifying WEP by utilizing TKIP enables superior security to WEP, nevertheless the most secure way to provide cryptographically secure communication is to use well known and studied standard encryption algorithms such as AES, and CCMP utilizes AES in cipher-clock-chaining mode to produce a MAC and to encrypt the message. WEP only protects against casual attackers and the new 802.11i will provide such needed wireless protection from malicious users.

VIII. SECURING A WIRELESS NETWORK

The paper advocates to design WEP technology with dynamic key support and essential certificates like enterprise root certificate, computer certificate and user certificate. The wireless policies must be configured like restrict access by user or computer identity, the domain or group the user belongs to, IPsec policies, wireless network (802.11) configuration and Access time. Creating security authentication methods able to use SSL and TLS tunnels.

Strong authentication in Wireless LANs such as EAP-TTLS ,EAP-TLS and PEAP authentication can be applied along with DES,AES and 3DES which are the cryptographic options for encryption.

Designing a secure wireless network with IPSec VPN which controls the access to intranet with the help of strong authentication method but cannot control the access of wireless card.

Designing a secure wireless network using 802.1x with EAP which also controls the access to intranet.

It also controls access to WLAN but needs more server than IPSec VPN. It also provide strong encryption by supporting dynamic WEP but its design is more complex than IPSec VPN whose authentication starts from data link layer.

Data encryption via AES-CCMP which is used in the 802.11i security protocol to restrict the key length to 128 bits. AES-CCMP incorporates two sophisticated cryptographic techniques such as counter mode and CBC-

MAC and adapts them to Ethernet frames to provide a robust security protocol between the mobile client and the access point.

AES itself is a very strong cipher, but counter mode makes it difficult for any eavesdropper to spot and detect patters, and the CBC-MAC message integrity method ensures that messages have not been tampered with.

Most of the security problems are envisaged due to human errors. Problem may trigger if users neglect their own private or critical information in the form of data leakage. Some crawler's bots can find the email address in web sites and mail spam to the users. This also intensifies the problem if some bots find the id of users as these all are important information pertaining to a network.

However, an event can always be recorded in the form of logs. An intruder's activities are recorded by the log files and log tools which can easily predict about the incidence occurred in the server or network. Network forensic tools can be applied to detect the attacker with the help of intrusion detection tools and log files.

Log files easily reveals about the ip address of the intruders and can also reveal the ports which are involved in the application.
Wireless threats are growing tremendously and hence to detect malicious activity on wireless network Wireless Intrusion Detection System, Wireless Intrusion Prevention System and Router logs can be incorporated as a regular practice.

Wireless Mac filtering can be circumvented by scanning a valid MAC and then spoofing one's own MAC into a validated one. This can be applied in the windows registry or by using command line tools on linux platform as a MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and white lists.

CONCLUSION

The proposal describes defense in depth with an integration of several security tools applied using an onion model on its various layers as a unified security system. The implementation of several hacking tools identify major security threats or vulnerabilities which an organization may encounter. Implication of proposed methodology that is simple and easy to adapt making it worthy to accomplish an internal risk analysis for organization which will definitely encourage more organization to implement internal risk analysis instead of seeking for auditing companies which could be an expensive and difficult to use. It also provides an offensive method toward the detection and prevention of any intrusion and can be used by IT administrator to study and learn intrusion nature and the attackers' mechanisms.

REFERENCES

[1] IBM Global Technology Services. , "White Paper IBM X-Force 2012 Mid-year Trend and Risk Report.," IBM Corporation (USA),(2012).
[2] Ali Jahangiri. , Practical hacking and countermeasures., USA: Ali Jahangiri Org(2009).
[3] Erickson, J.Hacking, The Art of Exploitation. 2nd edition., William Pollock(2008)
[4] McClure, S. Scambray, J. Kurtz G. , Hacking Exposed Network Security Secrets and Solutions. 7th edition(2012)
[5] Robert Schifreen.. , "Defeating the Hackers," Wiley , UK(2006)
[6] Christian Barnes, Tony Bautts, Donald Lloyd, Cric Ouellet, Jeffrey Postuns, David M. Zudzian and Neal O'Farrel, " Hack Proofing Your Wireless Network," Syngress (USA)(2002)
[7] Harold F. Tipton and Micki Krause. , Information Security Management Handbook. 6th Edition., Auerbach Publication (USA)(2007
[8] Thomas, S. R., Veitch, C. K. K. and Woodard, L. , "Categorizing Threat: Building and Using a Generic Threat Matrix.," Sandia Report SAND2007-5791, Sandia National Laboratories, Albuquerque, New Mexico(2007)
[9] Mark Mateski, Cassandra M. Trevino, Cynthia K. Veitch, John Michalski, J. Mark Harris, Scott Maruoka, Jason Frye, "Cyber Threat Metrics," SANDIA REPORT, Sandia National Laboratories(2012)
[10] Chris Roberts, ., " Biometric attack vectors and defences,," computers & security 2 6, Vols. Elsevier Ltd, , pp. 14-25, (2007)
[11] Eric Cole, Hackers Beware, New Riders Publishing, 1st Edition, ISBN: 0-7357-1009-0(2001)
[12] D. Lee, J. Rowe, C. Ko and K. Levitt , "Detecting and defending against Web-server fingerprinting," 18th Annual Computer Security Applications Conference, pp. 321-330(2002)Raymond, J. Panko. , "Corporate Computer and Network Security. 2ndedition.," PEARSON. (USA)(2011)
[13] Yuill, J., Denning, D., and Feer, F. , "Using Deception to Hide Things from Hackers.," Journal of Information Warfare., Vols. 5, No. 3, ., pp. 26-40(2006)
[14] Yinglei Wang, Wing-kei Yu, Shuo Wu, Greg Malysa, G. Edward Suh, and Edwin C. Kan., "Flash Memory for Ubiquitous Hardware Security Functions. True Random Number Generation and Device Fingerprints," 33rd IEEE Symposium on security and privacy (S&P 2012). IEEE computer society (USA). , pp. 33-47(2012)
[15] Youngho Cho, Gang Qu, and Yuanming Wu. , "Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks. IEEE CS on Security and Privacy Workshops.," IEEE computer society (USA), pp. 134-141(2012)
[16] Thaier H., Razvi D., Prashant K. and David T. , "Source—destination obfuscation in wireless adhoc networks.Security and Communication Networks.," John Wiley & Son Ltd (USA)., vol. 4, no. 8, p. 888–901(2011)
[17] Vivek Balachandran and Sabu Emmanuel. , "Software Code Obfuscation by Hiding Control Flow Information in Stack.," IEEE Workshop on Information Forensics and Security (WIFS). , pp. 1-6(2011)
[18] Mangasuli, Mr Sushant, "Hackers and Intruders: Motives and Difference.," International Journal of Electronics and Computer Science Engineering , vol. 1 no. 3, pp. 1446-1448(2012)
[19] Kevin P. Dyer, Scott E. Coull, Thomas Ristenpart, and Thomas Shrimpton. Peek-a-Boo, "I Still See You. Why Efficient Traffic Analysis CountermeasuresFail," 33rd IEEE Symposium on security and privacy (S&P 2012). IEEE computer society (USA), p. 332–346(2012)
[20] David Jacobs. , "How to perform a network security audit for customers," TechTarget Inc (USA)(2012)
[21] Wang, P., Wu, L., Cunningham, R. and Zou, C.C., " Honeypot detection in advanced botnet attacks.," Int. J. Information and Computer Security., Vols. 4, No. 1, p. 30–51(2010)
[22] J. Hu, X. D. Hoang and I. Khalil., " An embedded DSP hardware encryption module for secure e-commerce

transactions.Security and Communication Networks," John Wiley & Son Ltd (USA). , vol. 4, no. 8, p. 902–909(2011)

[23] Jung-Shian L., Che-Jen H., Chih-Ying C. and Naveen C. , "Improved IPsec performance utilizing transport-layer-aware compression architecture.Security and Communication Networks.," John Wiley & Son Ltd (USA)., vol. 4, no. 9, p. 1063–1074(2011)

[24] Rajesh K. T. and G. Sahoo., " A novel steganographic methodology for high capacity data hiding in executable files," International Journal of Internet Technology and Secured Transactions. (India), Vols. 3, No.2, p. 210–222(2011)

[25] Abdelrahman D. Sumstega. , "Summarisation-based steganography methodology," International Journal of Information and Computer Security. (USA). , Vols. 4, No.3, p. 234–263(2011)

[26] Hicks, M. Finnicum, S. T. King, M. M. K. Martin, and J. M. Smith. , "Overcoming an untrusted computing base. Detecting and removing malicious hardware automatically.," IEEE Symposium on Security and Privacy. IEEE computer society (USA)., p. 159–172(2010)

[27] Suman Jana, Donald E. Porter and Vitaly Shmatikov, "TxBox. Building Secure, Efficient Sandboxes with System Transactions," 32nd IEEE Symposium on security and privacy (S&P 2011). IEEE computer society (USA), p. 329–344, (2011)

[28] Fadia, A., The Unofficial Guide to Ethical Hacking.2ndedition., Canada: Thomson Course Technology , 2006.

[29] Christopher Wells, Securing Ajax Applications:Ensuring the Safety of the Dynamic Web, OREILY.ISBN 10:0-596-52931-7, 2007.Brian Komar, Ronald Beekelaar, Joern Wettern, Firewalls for Dummies, Wiley Publishing Inc. ISBN 0-7645-4048-3., 2003.