Global Information Assurance Certification Paper

Ethics for System Administrators & Security Professionals

Khurram Rehmatullah
SANS GSEC Practical
Version 1.4 – Option 1
May 2nd, 2002

Abstract

Today's world is a very different world. With new digital frontiers being discovered and conquered every single day it is indeed a full time job for system administrators to keep up with all the new technologies. However with these new technologies come new exploits and new vulnerabilities as well. And every smart system administrator must also keep up with all the new hacking techniques, and must always make use of the latest and most effective countermeasures. This brings in a question of ethics. Ethics for the security professionals is a subject that is not of recent born but is being paid a lot of attention in the industry nowadays. Some may say that corporations are beating around the bush and others may say that system administrators are beyond any suspicions. But the fact remains that too many managers have faced the wrath of disgruntled system administrators and too many corporations have been hacked with relative ease because of seemingly innocuous emails or messages that have been posted in the public domains by their system administrators.

So now the moods are shifting and the employers are proactively searching for personal qualities like honesty and integrity in their system administrators besides e-expertise. Of course one of the major criteria for all system administrator positions is the certifications they have earned, besides technical experience. So employers are now demanding their new hires to have certifications that mandate ethical behavior from the certificate holders. For example certifications issued by SANS/GIAC, which are revoked on the first instance of unethical behavior, like plagiarism. [1] This paper expands on the idea of the need for speed for all companies and corporation to be aware and become interested about the status of their present and future system administrators and IT personnel to ensure and insure their e-futures. The paper also explains some basic ways in which system administrators can abuse their position and authority. The paper finally ends with a recommendation for all companies who hire system administrators in order to maintain a healthy, trustful and fair relationship between the two.

Introduction

When I was fourteen I was persuaded by my father to enroll in a summer computer course. At the time, when all I really wanted to do was play ATARI games, I reluctantly gave in and attended those classes, which taught me from how to switch on my computer

(the good old IBM 8086 days) to some simple BASIC programming. Summarily it was fun and pain at the same time.

Thirteen years later after my graduation from University and having worked for a while, destiny threw me in front of computers once again. This time I was confident and I found the idea of learning and getting trained as a Network Security professional quite adventurous to say the least. My training started me off with the basic CCNA (Cisco Certified Network Associate) certification and then I was thrown into a waterfall of info about Windows 2000, Unix and Linux environments. I enjoyed (and still do) each and every moment and hungrily consumed and absorbed all the information that was tossed at me. I had read about hackers and had seen movies about hackers but had never even thought about becoming a computer security professional (a white hat) some day. The whole experience so far has been exhilarating and painstaking at the same time. My path towards becoming a network security professional made me realize and understand a lot of things about this profession. Like any profession, being an IT professional has both charms and pitfalls. This paper will illustrate how I came to the realization about the many pitfalls there are and how personal traits like integrity and sincerity are the only way to keep clear of the so many tempting traps that will come across any system administrator or IT security professional. If this paper succeeds in its objectives, then it will prove to be beneficial to both the managers and the system administrators alike.

Information Treasure Trove

While researching for the GSEC (GIAC Security Essentials Certification) practical I was exposed to the black hats. I had only heard about them before but for the first time I came across tangible information about the vulnerabilities of the millions of systems running all over the world and about the many who would like to do harm, their intention being just malice or just fun.

The wealth and depth of 'free' information astounded me. Even though most of the exploits and vulnerabilities that are freely available over the Internet are not '0-day', they are all useful one way or the other because of the many un-secured servers and networks that are operating using older software or without the right updates and security patches. Further, many websites even provide a list of known vulnerable servers and networks and provide interested visitors with actual IP addresses as well.

In a matter of days I was able to gather more than 15 toolkits from the Internet that helped exploit Unix and Windows environment systems. Many tools were multi-purpose for example Pandora by Simple Nomad and sponsored by the Nomad Mobile Research Center. They claim the following:

> **" Pandora is a set of tools for hacking, intruding, and testing the security and insecurity of Novell Netware. It works on versions 4 and 5. Pandora consists**

> **of two distinct sets of programs -- an "online" version and an "offline" version. Pandora Online is intended for direct attack against live Netware 4 or 5 servers. Pandora Offline is used for password cracking after you have obtained copies of NDS. [2] "**

Black Hats

It seems that the black hat hackers are indeed increasingly becoming a problem. More so than ever since the tides are shifting towards e-commerce. The availability of different exploitation tools is very tempting for the average e-cowboy, and the idea of being able to manipulate various systems and obtain user ids and passwords and to be able to invade and obtain the saved private information from the compromised system may be too voyeuristic a tempting for most. And above all is the most common reason for hacking, personal satisfaction. One can see this mostly in the defacing of web pages belonging to CIA, FBI and the Department of Energy to name a few.

One such hacker group, which calls itself F0rpaxe, says it is based in Portugal and takes responsibility for "massive attacks" on various Web sites. They sent a statement to Anti-Online saying**, " If the F.B.I. doesn't stop we won't, and we can start destroying. [3] "** They were of course referring to the extensive operations that the FBI cybercrime units are undertaking in order to bring malicious hackers to justice and to create awareness of the ramifications of such illegal activities.

E-Knights

That's not to say that we would be in a much worse situation if we didn't have help from within and without. Eric Baard, of the Royal Canadian Mounted Police Cybercrime Unit, gives us a good real-life example in his article. He says the following:

> **" Of interest, some sophisticated hacker groups act as watchdogs by alerting the government and other organizations to Internet security vulnerabilities. While their methods are controversial, their intentions are commendable. In May 1998, members of the hacker group 'L0pht' testified before the US Senate about Internet vulnerabilities. Several months before Y2K, a member of L0pht stated that he would publish a report on the Internet listing 30 US electric utilities companies which be easily 'shut down' by hackers if this sector did not fix critical computer based vulnerabilities. It is likely that L0pht had the capability to carry out this threat; however, the group is aware of the implications of such an exploit and did not have the motivation to deprive much of the United States of electrical power. [4] "**

Another major white hat source would be the U.S. government IT employees in different agencies like CIA, FBI and NSA and the various cybercrime units in almost every police department. All these people also keep a tight watch on everything that goes over information highways and say for example the chat rooms. These are the people who are the silent upholders of integrity and honesty because for them digital anonymity is almost always the case.

Of course, there is another group of people who are actively involved in preventing cybercrimes and who are also rarely recognized as denizens and protectors of the digital world. This group includes the network and system administrators, and IT professionals for the many LANs, WANs, etc all over the world. These people are actively involved in information theft prevention from their company databases and computers and in trying to maintain their employers' digital reputation and possible financial losses. However, just like in any other profession, system administrators also have the freedom to turn to the dark side.

The System Administrator

One of the most important qualifications for any system administrator is the certification he/she possesses. Many of the professional security certification organizations like Global Information Assurance Certification (GIAC) and International Information Systems Security Certifications Consortium, Inc. $(ISC)^2$ have recognized the need for creating and upholding a code of ethics for everyone whom they certify. $(ISC)^2$ state the following on their website:

> **" All information systems security professionals who are certified by $(ISC)^2$ recognize that such certification is a privilege that must be both earned and maintained. In support of this principle, all Certified Information Systems Security Professionals (CISSPs) commit to fully support this Code of Ethics. CISSPs who intentionally or knowingly violate any provision of the Code will be subject to action by a peer review panel, which may result in the revocation of certification. [5] "**

Increasingly, the industry is recognizing that these security professionals should definitely be required to follow a code of ethics. The security professionals they hire not only have the knowledge and the know-how, but also the tools to perform many of the hacks. Of course, these security professionals need the in-depth understanding of the past infamous hacks in order to safe guard their own systems and networks and/or the networks of their employers. And at the same time they become fully aware of all the vulnerabilities that are present or can be made available at the touch of fingertips. Gradually, more companies are becoming proactive in upholding moral standards for their system administrators and network security specialists or consultants.

Script Kiddies

One must admit that there is definitely a problem out there lurking beyond the digital horizon. The black hat hackers are not a myth but a reality and their existence has been proven beyond any doubts to everyone regardless of computer literacy. Who hasn't heard some one else tout about the damage caused by the infamous hacker of the 90's (and probably of all times—some may say) Kevin Mitnick.

Of course, most system administrators would tend to follow the traditional approach and would hound their employers for newer hardware and software thinking that this is all that's needed to maximize logical-security in their organizations. Usually they would raise a false alarm and quote the latest vulnerability surveys and end up hyping the actual risks up, in order to get the wanted increase in their annual budgets or to just get approval for bigger and better toys. One of the famous surveys that are readily quoted in the industry is the CSI/FBI Computer Crime and Security Survey.

Columnist Jay Heiser, who is a CISSP, pointed out the erroneous ways in which this particular survey is performed in his April 2002 article in the Information Security magazine. He explains that the major problem with such a survey is the methodology used for gathering the data necessary to compile it into useful tables and charts. According to Heiser:

> **" The creators, respondents and recipients of the study have not-so-hidden agendas. Survey respondents are asked to provide unsubstantiated estimates on the cost of computer crime, the results of which are processed and returned to those same people for use in support of their own agendas. See anything wrong with this process? The survey is purportedly published as a "public service," but a more realistic explanation is that it's a marketing tool for CSI, the FBI, enterprise security departments and infosec vendors. The FBI needs cybercriminals to justify the existence of its sexy computer crime units. Infosec officers want to increase their staff and responsibilities. Vendors use the statistics to drive sales. If you don't believe me, try doing a Web search on "CSI/FBI" to see how many security consultants and vendors cite this report as evidence of the need for their service or product. [6] "**

Social Engineering

I am not downplaying the need for better hardware and software since the Intrusion Detection Systems and the firewalls and the Access Control Lists: all play a significant role if the attack is from a script kiddie or a relatively low–tech hacker, who are usually teenagers, generally between 12 and 16 years [7], who mount an attack on a system sitting

in their bedroom using their personal computers using tools and scripts gathered from the Internet.

However, we must realize a balance and understand the truth. The hottest IDS and the best firewall in the market will, at best, only slow down a seasoned hacker. Most experienced and successful hackers employ a lot of their 'social engineering' skills instead of hardcore hacking alone, which can be easily (or with difficulty) logged and traced to the perpetrator. Even Mitnick's pet technique was social engineering. In an associated press article that was posted on March 2nd, 2002, New York Times quoted Mitnick warning lawmakers and senate panel members as follows:

> **" … about his favored technique of "social engineering," or deceiving others into believing he could be trusted. He told of duped victims at major corporations volunteering their passwords and even sending him secret software blueprints. "I was so successful in that line of attack that I rarely had to resort to a technical attack," Mitnick said. "Companies can spend millions of dollars toward technological protections and that's wasted if somebody can basically call someone on the telephone and either convince them to do something on the computer that lowers the computer's defenses or reveals the information they were seeking." [8] "**

Security Culture

Essentially, information security is not comprised only of technological superiority but should be treated as a culture within organizations and its employees. All employees should be security conscious at all times, and thus assist their security departments in thwarting hacking attempts. But, how can one thwart a hack from the very system administrator who is protecting them? Herein lies the ultimate problem.

System administrators have traditionally enjoyed, and still do, a position of inherent trust and confidentiality. They have the knowledge and the authority to monitor any and every activity for any user in their domain. So it becomes extremely important for them to adhere to a code of ethics. $(ISC)^2$ have laid down some basic Code of Ethics for their certification holders. They condense the above-mentioned principles on their web site and state the following [9]:

Code of Ethics Preamble:

- Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this code is a condition of certification.

Code of Ethics Canons:

- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

Admittedly the position of system administrator is indeed one of power. Usually they not only hold the keys to all the accounts on the network but they also have access to the logs that are generated automatically recording all activities over the network. These log files are not easily accessible since only a select few have access to them and usually these files are hosted on relatively more secure systems. However the system administrators can easily modify these logs since they usually have complete access to them. Not to mention there are plenty of tools available freely to 'fix' the logs, as one wants them to be.

I will explain some of the ways that system administrators can abuse their authority and access-rights and can potentially do a lot of damage to the network or the user.

IP Spoofing

One of the ways that system administrators can abuse their authority is by spoofing the user's ip or MAC addresses with relative ease. Usually this kind of spoofing (falsifying) requires root access or system administrator privileges on the system. So it is quite a straightforward task for the system administrators to hack the very machines they are responsible for and use the new 'false' account to mount an attack on some other system.

Since "IP spoofing" cannot be used to hide your IP address (for example: while surfing the internet, using email or chatting on IRC etc) therefore this is the next best thing for system administrators i.e. to create a new account with all the privileges they would need in order to do whatever it is that they intend to do using this account. Even if the attack is going to be a blind attack, root privileges may still be needed to run some of the required commands. Therefore it is simpler for the system administrator to just create an unauthorized 'guest' account with root privileges.

Countermeasure

Install software that manages logins on every system. Every time a user logs on to the network, this software should message the user and indicate the time and date for the last successful login. This information should be stored in an 'absolutely' read only file or an encrypted file and the decryption of the file should require the private key [10] of the user. This would safe guard the information within the file from any prying eyes.

Above all, corporations and companies should encourage a security conscious culture within the organization and encourage reporting of anomalous behavior or messages within the user's machines.

Password Cracking

For the system administrator who doesn't have the privileges to create new accounts on the domain there is yet another technique. Usually such system administrators will at least have the authority to edit user accounts and reset their passwords in case of forgotten or lost passwords. These system administrators may also have access to the file in which all these usernames and passwords are stored. Hence they can easily copy this file to a floppy and crack it later at home using any of the many password cracking tools available over the Internet such as L0pht Crack 3 (LC3) by @Stake [11]. As a matter of fact many organizations have a password auditing policy and their system administrators are required to perform password audits on the user's passwords and inform the user in the case their password is compromised. Therefore once the user password is cracked the system administrators would have access to user's passwords and unless the program is automated to send an email to the compromised user account, it is up to the system administrator to inform the user to change his/her password. Until the user changes his/her password, the system administrator technically has full access to the user account as the user him/herself. Consequently once an 'outsider' has accessed the user's account, digitally impersonating the user, all the intruder needs is a few minutes to install a backdoor into the user's roaming profile or on the user's machine itself.

Another easy technique would be to create a Hotmail or Yahoo free email account from the user's machine using the user's credentials. Now the system administrator will have a free email account that he can use to electronically send anything out to anybody in the world or to forward a worm or virus to the internet world at large, and in the case that it is ever discovered and investigated then the blame (at least initially) would fall on the innocent and ignorant user.

Yet another misuse of such information would be for the system administrators to abuse dial-up accounts. One can misrepresent his/her own MAC address and use the dial-up account of one of the user to 'freely' surf the Internet. In this manner the system administrator has no accountability for viewing or downloading any offensive or unauthorized or illegal materials from the Internet since it would leave no trace in his/her name and even if there were to be an investigation, the fall guy would be the unaware user.

Countermeasure

This is also preventable if user awareness is increased about the access into their network or remote accounts. Once again we come back to the concept of security being a culture in an organization. Every time users log onto the network they should always be made aware of their last login status and they should keep a vigilant eye on the date and time of their last login. This would prevent (or catch) any hacking attempts by system administrators or from any outside hacker. In the case of attempted hacking, the users should always change their passwords immediately and in the case they don't have authority to change their own passwords they should be able to get their account or password 'reset' and should be encouraged to report the hacking attempt to appropriate authorities.

CD/DVD Ripping

These days a major waste of company resources happens in the form of CD/DVD ripping. Such CD or DVD ripping tools (usually for music and movies respectively) are easily and freely available over the Internet. The average user is hesitant to perform such tasks on his company laptop or desktop because of his/her fear of being audited some time in the future. However, system administrators are usually deemed beyond any doubt, not to mention that they would be the ones to have access to the right logging files (for editing purposes) while the individual user doesn't. Hence it is simple for them to delete any such logs that are created due to misuse of company assets, in both company hardware and company time, surfing the Internet or abusing copyright laws.

Unfortunately this is a growing problem. Many managers opt to be quiet about system administrator abusing copyright laws on his company computer as long as work is getting done. However, what most managers do not realize are the implications if the system administrator is caught with such material/evidence on his company provided computer. The organization itself (in some cases) can be held responsible for such abuse of copyright and proprietary laws and can be held liable in a court of law. One aspect to be clarified is that it is not entirely the manager's fault. It is indeed a growing and tempting trait in system administrators to feel as if the law does not apply to them since they are the upholders of the law. Since most system administrators have the responsibility of keeping an eye on the users to prevent any copyright laws from being stepped over, it is common for them to feel above the law and think that they will never get caught.

Countermeasure

Surprise audits of the system administrators' laptops or desktops should be part of company policy and tradition. Each and every organization should uphold copyright and licensing laws towards all of their employees specially the system administrators.

Backdoors

This is by far the most common concern of managers in the IT world. Every manager knows (or should understand) that their system administrators may have back doors installed in their systems. These back doors can have two common forms of either an extra user account with system administrator privileges or a hidden back door to access the system by running a specific command at system level. To system administrators, this back door is like the gateway to salvation in the case when everything goes wrong and even they themselves are locked out of the system. It is this dark day that every system administrator fears and its because of this justification that most system administrators rationalize the installation of a back door in their system (even if this is against company policies) that only they have the key to.

Of course for the managers this is a nightmare since installation of this backdoor means that the system administrator would have access to the system as long as the system is up and running. This is particularly troublesome for the organization, since it means that the system administrator would have access even if his/her job was terminated. Also if by chance a hacker found this backdoor then he/she also would have complete access to the company proprietary information.

An even worse nightmare for a manager is if one of his system administrators installs a time bomb in the system. These programs require some steady input in order for them to stay dormant. This input can usually be of the form of the system administrator logging on to the network. Therefore the time bomb would activate only in the case that he/she didn't log on to the network for say a whole month. Once activated this time bomb is unstoppable and would result in at least major disruption of computer services and in more drastic scenarios could also end in complete system obliteration.

Once again there are plenty of tools available over the Internet to do just this. The system administrator can use these tools to actually install a stealth back door that unlike a regular account does not show up in regular audits. Such back doors even allow remote connections and since the account has root privileges, the system administrator, once remotely connected to the system, can run/install anything on the machine and he/she has the potential to do a lot of harm.

Countermeasure

Special logging software should be used and singular attention should be given to any remote connections that are established out of the ordinary. All software installation records should also be kept safely for auditing and if possible the main system should be configured to require dual authentication for both installation and uninstallation. Another easy technique for the managers is to ask different system administrators to perform an audit each time and specially in the case where there is only one system administrator then the responsible company

should look into getting an outside independent auditor to carry out a surprise audit on their system looking specifically for such backdoors and Trojans and time bombs.

Recommendations

There are several recommendations that can be applied towards the build-up of a sound security culture in any organization. This culture generally should mandate a check kept on all cyber activity and strict adherence to company security policies, and no one should be considered above the law including the ever-trusted system administrators.

Self-Policing

Self-policing is imperative for all system administrators. They should possess not only the necessary certification and technical experience but should also enjoy being honest and trustworthy and safe keepers of confidential information. It is crucial that system administrators should not consider themselves above the law and should always practice what they preach for example copyright laws. At the same time organizations that employ system administrators should also help the system administrators keep straight by employing preventative and policing measures themselves.

Smart Cards / Biometrics

Smart cards and biometrics (whether alone or combined) are winning new grounds in the security world for the individual user. Smart cards have built in memory cards (that cannot be easily hacked with current technology) that can hold digital certificates, encryption private keys and the user's unique personal identification number etc. By utilizing smart card logins the organizations can safeguard the user computer from any snooping system administrator since having the PIN of the user is not enough for the system administrators to access the user's computer, the smart card itself is needed as well. Of course smart cards have an additional advantage of being utilized as picture ID and of being relatively inexpensive.

Biometrics is another technology using which only the individual user has access to his/her computer. So far biometrics include voice, finger and hand printing and retina pattern recognition. Since these characteristics are unique for the individual, the private data and resources are once again safeguarded from any unauthorized access or intrusion. Of course the biometric technology can be combined with the smart cards in order to further secure the authentication process.

Zero Tolerance

Many companies only look as far as certifications held by the individual when they are considering him/her for the system administrator position. Organizations should try to look beyond the certification level of the individual and look at the big picture. They should try to hire individuals who have a well-rounded personality and who actually enjoy following, enforcing and improving rules and policies and who have at least graduated from an accredited university and have interfaced with more than just their friends over the IRC.

In addition the system administrators and all other employees alike should also be made aware of the zero tolerance policy that organizations must start to exercise towards increased e-security. Especially, system administrators should be made aware that their illegal behavior, regardless of how minor it is, would not be acceptable. And that these actions would be immediately reported to appropriate authorities and exacting actions would be taken against any one who is found to be the perpetrator beyond any doubt.

The last but not the least practice for companies in order to keep the system administrators in line would be by introducing surprise and mock audits among their employees including the IT staff.

Resources

System administrators are part of the IT resources for the organizations. Managers should always be mindful not to overburden the system administrators. If the system administrators are over-worked then there is the possibility of them missing out on finer details that a hacker may not overlook. A possible answer to this can be as simple as hiring more system administrators in case the work is exceeding all projections. This may not look good in the accounting books; however, there are a couple of advantages. Firstly the system administrators will have more help and more time to really improve security policies in the company. Task like revising the firewall's current rule base requires a calm and worry free mind. Secondly, more than one system administrator has the additional advantage of implementing checks and balances within the IT department. Therefore, adding to the system administrator staff may eventually be a benefit to the organization in terms of increased efficiency, improved security and checks and balances in-between system administrators.

Conclusion

So the first step for any organization is to realize the risk they may be facing if they are not implementing security procedures for their IT staff. Instead of worrying about

Trojans from the Internet and email the managers should be wary about any Trojans within the organization.

This paper has listed some basic techniques that the malicious system administrator may utilize in order to further his gains. Therefore the organizations should start practicing preemptive measures to ensure that their network is not compromised from within. In keeping with my previous recommendations, employers should emphasize about personality traits like integrity and honesty in their system administrators and not settle for IT skills alone. Additionally, companies should do extensive background checks on their system administrators, including, and not limited to, calling previous employers, acquiring their criminal history, if any, and looking for patterns in their job history such as job-hopping.

This would help the organization save money by reducing the possibilities of lawsuits in future and by increasing worker efficiency. Organizations will have to move slowly towards zero tolerance as their policy and greater than ever expectations from their IT staff.

Also they should encourage certification organizations like GIAC/SANS and $(ISC)^2$ by requiring the IT security employees to obtain certifications from them since these organizations help keep a vigilant eye on all certification.

The recommendations and solutions provided in this paper are by no stretch of imagination the final conclusion to the outlined problem. As long as there are computers and networks there will always be a need for system administrators and IT security professionals and as long as there are information security personnel there will always be a need for them to exercise first-class ethics in all things that they do.

References

[1] GIAC Certification Administrivia for All Assignments, Version 2.1. http://www.giac.org/admin_21.php (2 May. 2002).

[2] Nomad Mobile Research Center's official Pandora website. http://www.nmrc.org/pandora/index.html (2 May. 2002).

[3] lists.jammed.com mail list archive. Info Security News. June 1999. http://lists.jammed.com/ISN/1999/06/0006.html (2 May. 2002).

[4] Baard, Eric. "Hacker: I Can Black Out 30 US Electric Utility Grids." Criminal Analysis Branch, Royal Canadian Mounted Police. May 30, 2001. http://www.rcmp-grc.gc.ca/crim_int/hackers_e.htm#6 (2 May. 2002).

[5] International Information Systems Security Certifications Consortium, Inc. http://www.isc2.org/ (2 May. 2002).

[6] Heiser, Jay. "Can you trust infosecurity surveys?" Information Security Magazine. April 2002. http://www.infosecuritymag.com/2002/apr/curmudgeon.shtml (2 May. 2002).

[7] Benton, David. "What's Inside a Cracker?" SANS Institute web site. November 28, 2000. www.sans.org/infosecFAQ/hackers/cracker.htm (2 May. 2002).

[8] The Associated Press. "Noted Hacker Speaks Before Senate Panel." The New York Times. March 2, 2000. http://www.nytimes.com/library/tech/99/mo/biztech/articles/02hack.html (2 May. 2002).

[9] $(ISC)^2$ Code of Ethics Preamble & Canons. http://www.isc2.org/cgi/content.cgi?category=12 (2 May. 2002).

[10] Sol, Selena. "Public Versus Private Key Encryption." September 20, 1999. http://www.wdvl.com/Authoring/Tools/Tutorial/public_vs_private.html (2 May. 2002).

[11] L0pht Crack 3 password cracking tool by @Stake. http://www.atstake.com/research/lc3/index.html (2 May. 2002).