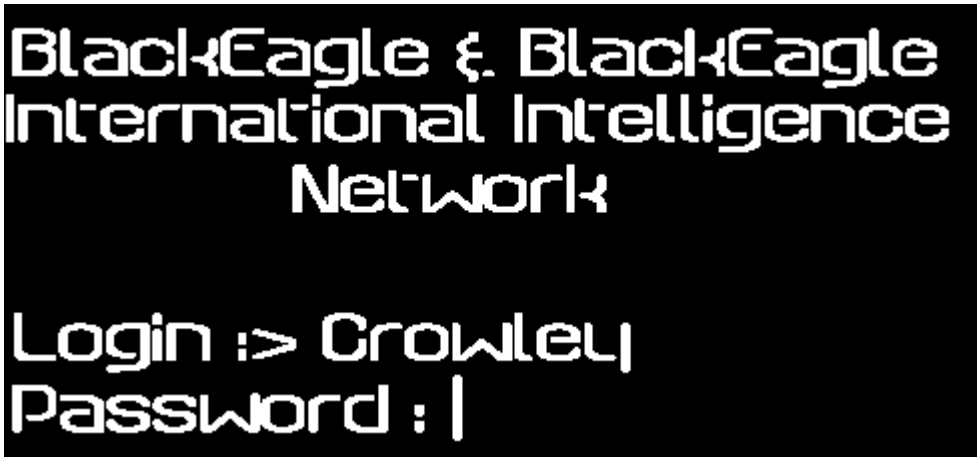
Crowley's (quick) Guide to the Net.

Aleister J Crowley's guide to hacking on the GenNet in 1999.

Written by Crowley
AleisterJCrowley@rocketmail.com
http://www.fortunecity.com/tattooine/blish/152/
http://www.fortunecity.com/tattooine/blish/152/Crowley.doc

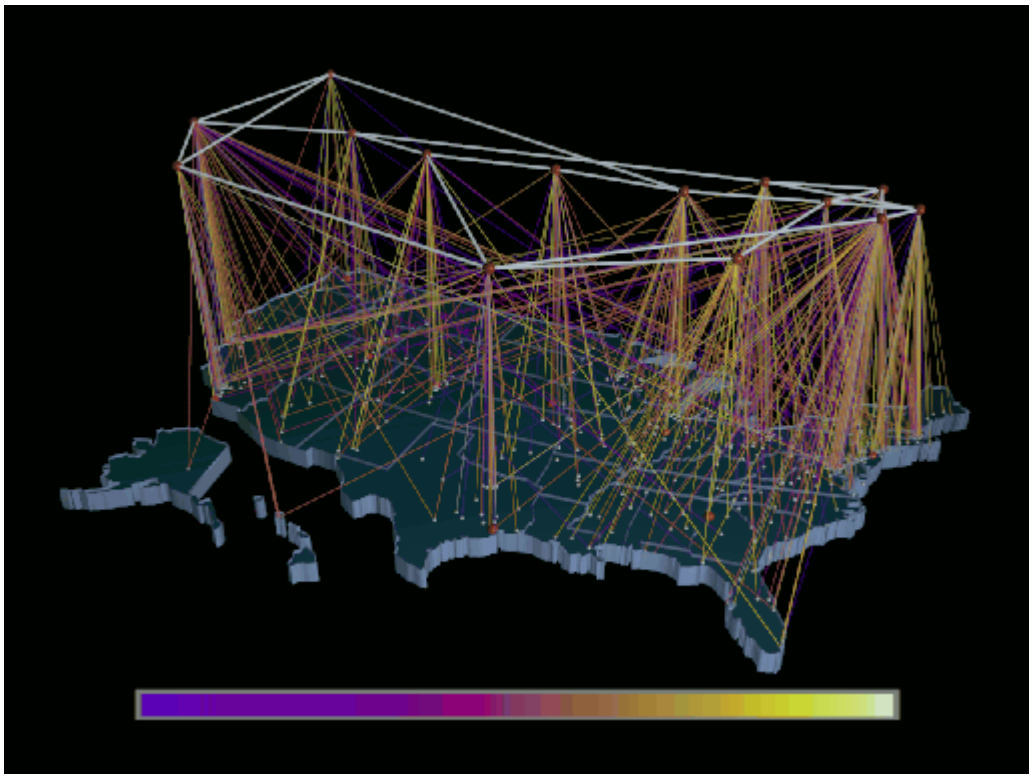


This guide is simply a way of expanding and fleshing out the GenNet rules in Milleniums End. So far I have avoided system diagrams, as these are relatively irrelevant, this is simply a guide to types of systems, and methods and tactics used by successful hackers.

This guide will be broken into several parts:

1. What the net is, and how it is built up
2. Some common ways of accessing the net
3. Types of system attached to the net
4. Getting into systems, and using them
5. The Enemy
6. Some tools for the above
7. General Hacking notes
8. Some other tricks for a hacker character.

Chapter 1: the GenNet itself.



In the diagram above, the lighter the shade of the line, the higher data flow.

The GenNet is an extension of the world-wide computer network known as the Internet, now defunct in 1999, replaced by higher speed optical fibre networks and purpose built video and audio feeds, running alongside standard data channels. Just as the Internet evolved, so has the GenNet, originating in the US where higher capacity data transmission was demanded, and without the traditional restrictions put on it by the Phone companies, with the capability of running audio and video across data channels while being able to encrypt it more effectively than before, and with greater depth and use, the ability to transmit high quality images alongside normal real time text communication. The GenNet is built essentially on the same lines as the Internet, running across high bandwidth fibre optics, standard phone lines, satellite links, microwave and radio. The GenNet is becoming as lawless as the Internet as well, with little or no overall control, and this is set to get worse as the GenNet expands across International boundaries, with Europe connecting major systems to the GenNet, as well as military organisations across the world. There is now a larger element of registration of the Net, using lists of connection codes and addresses linked to descriptions and terms

of usage of each computer connected. Although many systems are not registered in this way, it makes finding simple sites of information a lot easier.

The usage of standard communication set-ups for transmitting information on the Net means than actual physical tapping of lines is very, very easy, so it is essential that encryption is used throughout the system, unless of course it is insensitive information being transmitted, but as we all know, most people think their information is important! Even with this basic encryption, the use of methods on top of this is advised. There are also rumours that these basic levels of encryption that are used on the simple transmission lines have had "back doors" left in them to allow the security forces to be able to listen in on supposedly safe traffic.

The simplest way to look at the GenNet is the Internet, just juiced up, and slightly more organised (but not however, as well administrated), and with far more capacity as it has had up until now. In fact, the GenNet runs off old InterNet routes, but has just expanded and improved on the original setup.

Chapter 2: common access methods.

The most basic method of accessing the net is by using a desktop or laptop computer, the basic PC with a GenNet access card, either connecting to the nearest GenNet access node through cellular phone connections, or using the physical phone lines. There are various software systems for accessing the Net, giving hypertext browser access, Telnet access (when you actually operate the computer system you're connecting to rather than just the data on it) file download access, and Integrated System Access, an innovation possible through the GenNet's development from the Internet, where high bandwidth systems can transmit their results to a remote system, for instance, a buildings security system attached to the GenNet can be accessed by a remote user, who can operate the buildings systems, and view the security cameras signal across the system. This sort of access, whether obtained legitimately or not is invaluable to a BlackEagle cell. Many smash and grab raids on private institutions can be made far easier if the buildings security system is made deaf and blind by a resourceful hacker.

The ability to synchronise normal textual system prompts with video and audio feeds makes a great deal possible, but there are still limitations imposed by bringing together so much information, often through several different data feeds, especially when using a mobile set-up, using a laptop computer with an encryption system and several re-routings of signals to make a trace more difficult can slow down many systems, probably not to seriously degrade a signal, but definitely to make any usage of a connection more efficient by necessity.

Saying this though, a hacker should be using only the bare minimum to get in and out of a system, and she should take only the least amount of time required to perform any action. A BlackEagle hacker won't be the traditional social outcast, operating from a bedroom full of computer junk, like the hackers of old. BlackEagle hackers require a greater range of skills, because the hacker mindset includes rapid problem solving skills, and often technical knowledge, a cell's hacker may well have lock-picking skills, almost always specialising in electronic locks, but with a small amount of miniature engineering skills, enough to break most common locks, and to disable common electrical alarm systems, at least, the ones he has failed to disable through breaking a company's computer systems. Hackers are very likely to possess a great many contacts in these areas as well, as their community tends to stick together, even though many hide behind handles and code names they give themselves, almost everyone will have the skills required, or know someone who may have them.

Among the common access methods, many hackers write their own, so expect to find variant on common software packages designed for more specialist applications.

So, in summary, the main access methods across the GenNet are :

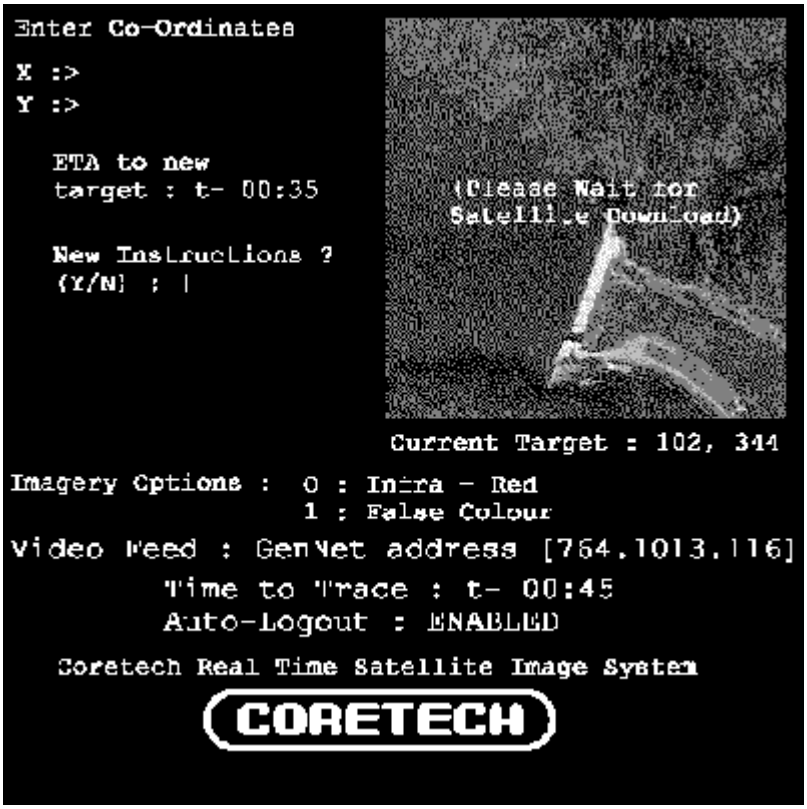
Browse : similar to Netscape/Explorer access, gives the user easy and simple use of hypertext documents, providing complex documents including video/audio formats, overlaid text feeds, and intelligent Net mapping software, recording a users trips over the net.

A typical Public Lobby screen - basic public information pages, followed by remote user access, available only to legitimate InGen users.

Session : the old Telnet software has been updated for the GenNet, capable of running sessions connected to many different formats of system, getting past the standards barrier that restricted the Net in the past. Most versions of Session software just connect to a GenNet address, but many modified copies now have the capability to route through systems to cover their tracks, and make any trace far more difficult. Any options like this are completely interactive, so the hacker knows how many connections stand between her and her target, and across which physical tracks they travel as well. Session essentially allows the user to connect to a computer, and use it as if they were sitting at the keyboard itself, running software on the target machine, and due to the higher bandwidth capability of the GenNet, even run graphic intensive programs on the remote machine. The user may only be given a small amount of access using Session software, because of the degree of freedom Session programs give the user.

File : This is a swift and efficient file retrieval software system, connecting to a certain system, and displaying libraries of files available, with descriptions, sizes, file types etc. This system has hardly changed since its first incarnation as FTP on the Internet.

Mail : most mail is held on large remote servers rather than the users personal machine now, this is mainly to facilitate the use of the Net-Card, a personal smart-card, containing a users mail verification code, to allow the user to read mail from specialist phone booths with GenNet connections without the rigmarole of going through password verifications, and logging in to mail servers and services. This card has many other uses, as I'll go over later.



An example of an Integrated System Access screen.

Integrated System Access : The most sophisticated access system. This uses some dedicated programs, as well as integrating some of the above programs, to provide a user with direct access to a computer system, and then overlay that with audio and video feed from other computers from a network for instance, or from other feeds connected to that computer. This is commonly used for entertainment systems, giving video/audio overlays with a film library, or just plain audio with music libraries, or to tourist archives, with footage from towns and cities integrated with tour guide style soundtracks alongside descriptions of places and sites of interest. The system is not unlike Browse in the information available, but is much more powerful in the manipulation possible to the user. Control of physical systems such as robots and cameras has been tried before but suffered from the low bandwidth of the Internet and suffered because of the feedback time from telling the robot to do something, and seeing that it had done it. Many systems now have libraries of graphics to represent the information held on them, for instance graphical user interfaces of lift systems would be available to building administrators to use their own system, and because the mechanics are already there, it makes it easier for an outside user to use an intelligent system.

For an example of an Integrated System Access session, imagine a console screen with a list of cameras available, and a text based system allowing the user to input movement commands and see the effect of these commands on the video feed. There will usually be a manual of sort on-line for lists of commands available, this is true of most systems.

All of these systems exist in many versions, with variations in the software, but sticking to the main functions listed above. Many modified versions exist with functions specifically written for the hacker, including re-routing, encryption, and password/ice breakers.

All of these systems are the basics to entering the GenNet, many other tools exist, but the most useful tools for the hacker will be described in chapters 4 and 5.

Chapter 3 : Types of system attached to the Net.

There are several large systems included in the GMs handbook, including a building control network, a corporate net, and a police net. These are fairly specialist networks, but are typical of the networks accessible, and *very* typical of the type of network a BlackEagle hacker may be expected to get into.

The GMs handbook makes it clear that once a user has control of the network Administration Computer, then he can avoid the security rolls required to get into some of the more important machines. This is easier said than done however, requiring a security roll at -60 to get from the lobby computer to Admin, and then a civilian systems roll at -80 to access the data entries that give you access to the rest. This means that with a civilian systems skill of 80, you still have to roll under 0, errrrm, a teensy weensy bit difficult.

But it *is* worth the effort, if you control Administration, you can lock everyone out of the network, access any machine on the network, and have free reign over the network. You *rool*. These rolls may be modified by the use of tools written for the hacker, check chapters 4 and 5 for these.

Some good examples of systems attached to the net of interest to the hacker are :

1. **Government databases.**
   These range from large complex central government systems such as the IRS, and other large domestic services, to small local government databases, schools, hospitals etc.
   The security really will depend on the size of the system, and the importance of the data contained on it. There will usually be a fairly good level of security.

2. **Municipal Control Systems.**
   Electrical, Water, Sewage systems, albeit fairly primitive systems, may well have public information systems attached, and connections for administration and evaluation purposes for use by local government and inspection services. These are likely to have fairly robust but unimaginative security on them, and usually government evaluated and approved security at that.

3. **Law enforcement.**
   A police system was outlined in the GMs handbook. These will have fairly heavy security on them, but fewer competent personnel to enforce this, so timing is a major factor in the penetration of such systems.

4. **Phone and cable companies.**
   These are the holy grail sites of the hacker world. A hacker that can get into the large companies systems, especially the administration computer, is a celebrity in the hacker community, these systems are large, very secure, and have some of the most complex security imaginable, someone who can get into these, can manipulate phone systems, set up complex re-routing of calls, and modify records to erase records of calls, or manipulate such records. Finding ex-directory numbers, government lines and the usage of such lines is also possible. Expect very high negative modifiers to security rolls on these sites, and expect a large group of heavily built men breaking your door down if you screw up. (so don't screw up!)

5. **Government Agencies.**
   Law enforcement, including the FBI, CIA systems are all connected, but expect security rivalling the phone companies', and expect a bullet in the head for any errors you make. BlackEagle's rivals also run systems comparable to these, and with less legal recourse when a computer intruder is detected too. (which means they plump for the ole bullet in the head trick, funny how techniques crop up all the time in this field)

6. **Corporate nets.**
   We've already seen these in the GMs handbook, but these can have a lot more connected to them than just the basics. Corporate nets have a lot of unmapped connections. For instance,

from a corporate net, you may well be able to connect to a corporate communication system, including satellite comms, and even television feeds.
A companies entire history, strategy and finance is available on this system, so make sure you're quick in and out, coz these mothers have some heavy duty security on some sections.
Some corporate nets have the building controls as a subnet, so an infiltration mission with a physical element can be more easily completed from one of these nets, providing the headquarters is the target, any building system is going to be connected to the computers nearest to it in physical terms.

7. **Military systems.**
Well, the basic plan is *don't bother*, however, if you do, make sure you don't leave a trace, there is a lot of info on military systems, and a lot of it is highly classified, expect difficult rolls, and a hell of a lot of payback, good or bad, it tends to go a long way in either direction. Try and dissuade your players for going out and hacking the US nuclear launch codes, they're hard to get, and worth bugger all when all is said and done. (five minutes after you hack them, they'll be changed, etc etc. The safest thing to do is just stay away from these unless the assignment requires such drastic action. However, knowledge of these systems is useful in any assignment which involves military espionage.

Chapter 4. Getting in, and getting out.

Step 1 : Identify the information you require, and whether it is available on the GenNet, and if it might be easier to discover through other channels. Decide on the action required once this information has been found.
This may sound stupid, but in some instances, hacking across the GenNet may be the last resort, always bear in mind that some information may be more easily found elsewhere. (see Social Engineering in the last section)

Step 2 : Identify the system that this information may be stored on, and the GenNet address of this system
The most basic step is to find the GenNet public access address, many of these are publicly available, however, some may need some research to discover. There is always the possibility that the system you need to hack is not connected to the GenNet, or a public phone connection, so the Cell may need to break into the building where the computer is, to gain physical access to it.

Step 3 : Connect to this system.
This is best done from an anonymous GenNet address, preferably using a cellular connection, and a mobile location if possible. To get the information, the use of some hacking software may be required, otherwise the rolls required in the GMs handbook stick. For other methods, check out the last section of this document, for phone phreaking and other games for the hacker to play.

Step 4 : Download, or modify the information.
Use Scan (described later) to find the required files, use standard software to move them to your local system. Once the first 3 steps are completed, this should be fairly simple. In case of capture, or investigation, come form of encryption will be useful when storing this information locally.

Step 5 : Disconnect from the system cleanly.
Just shutting your computer off, or pulling the phone cable out of the wall may sound fairly sure fire exit methods, but don't get carried away, once connected, the target system records your GenNet address for the period of the connection, if this is broken for any reason, that address may be kept in memory for a short time, so actually taking a few seconds to safely log out of a system is a wise precation.

Step 6 : Leave your current location.

A Trace does not show up on the hackers computer, so there is now way of knowing whether your location has been compromised without serious telecommunication hardware.
If using a mobile cellular link, your actual physical location takes longer to make a fix on, but due to the possibilities of hacking, for a fee, telecommunication companies can provide fixes on transmission locations to corporate users, the military and selected individuals (for a price).

Some hacks may be made to disable a computer, some to obtain information, and some to modify data, a great deal of planning is required for the latter, because any modification of data can be seen by its relation to other data on the system, there are cross references, and indexes which need to be maintained, so the hacker must bear this in mind.

Chapter 5. The enemy; the systems, and the programs used to keep you out.

A typical system administrator, SysAdmin for short, will have very high computer skills, almost all subskills totalling 80+, or more dependent on the amount of time they have spent in the industry. A SysAdmin's job is to keep a system running smoothly, and to keep naughty little boys like you *out* of their system. SysAdmins are quite capable of writing complex software systems, to block the hackers entry into a system, but a few common programs are listed at the end of this chapter. A Hacker may even be an ex-SysAdmin, but may not have the high skill values appropriate to one, especially if they are starter characters. Of course, these skill values reflect *good* SysAdmins, and are subject to the same variations discussed at the end of this sourcebook.

Good systems, that expect some form of attack, protect themselves from attack by using a layered structure, that is, one obstacle, followed by another. Other techniques include puzzling the hacker, by hiding important data or files in the midst of irrelevant and unrelated material, or by putting data in places they wouldn't expect.

Some of the systems in the GMs handbook follow a system, whereby as soon as the hacker manages to bypass the systems lobby computer, they can attempt to connect with the Administration system. The best defence from an outside attack is to have the administration machine furthest away from the companies GenNet connection, and use a specifically built machine to protect the network from the lobby computer. The Administration computer, as we have said before, is the key to an entire network, break into this, and you have control of the entire system.

Some example programs ;

Trace : This operates in exactly the same way as the trace program discussed in the *Toys* section of this book, once the SysAdmin knows the username being used on the system, he can run this program, with 60 or more in the Networking skill, the user can be traced to his or her location in 5 minutes. The longer a user spends on the system after this first roll, the difficulty reduces by 10 every 15 minutes.

Block : Block is a simple but effective password program. Unless the user has the right password, they cannot access the system. This program can be circumvented with a security skill of 70. But use of a breaker program may make the roll easier. It requires a Security and Network skill of 60 to install properly.

Steg : Steganography is the tactic of hiding data within picture and sound files, or by coding data to resemble something else, i.e. a text file into another text file that reads like a normal text file, albeit on a peculiar or completely irrelevant subject. Steganography can be bypassed purely by checking sound files, and pictures for this type of security, this takes some time however, but it is an effective way of hiding sometimes very important data in the open. It takes a security skill of 50 to find a file stored using this method, however, a file can then be encrypted using another method. To store information this way, a programming skill of 50 is required.

Encrypt : Encryption is one of the most popular methods of protecting data. A hacker might be able to obtain the file, but being able to read the enclosed information is near impossible without a password or algorithm to decrypt it. There are many encryption methods available, and a cracker for almost all of them. A Programming skill of 70 is required to identify the method used, and a security skill of 60 on top of this to decrypt it.

Scan : A simple program to watch a system for irregular access. If a user performs actions they would not normally be performing, this program alerts the sysadmin. A common program on many mid-level and above systems.

Crash : This program can only be run after a successful Trace. Once run, it locks up the target computer, and crashes it. Simple and effective. Requires a network skill of 60, and a security skill of 55.

Flash : an almost mythical program, which is reputedly able to overload a target computer, and damage its hardware. In reality, it is a modified version of Crash, written by a military hacker. The few versions that can be obtained include a virus that deletes the program after one use. This also leaves a marker flag, and if a backup copy of flash is run, it will delete itself if the flag is found, and also hunt down any local copies it can find and delete them as well, this is to ensure that even if a copy of Flash makes its way into the public domain, any copies are restricted in the damage they can cause in a limited amount of time. It requires a security skill of 60 and a programming skill of 70 to run properly. A successful Trace also needs to have been completed. Effective use of Flash can be helped by running Crash against the target first.

Once activated, it will crash the target computer and set up an internal feedback loop, which can, if the computer is not swiftly disconnected, damage the most power sensitive components of the computer. This will not have any effect on the hard drive of the computer, however, some modifications to Flash include virus systems to be injected into a target computer before it crashes it.

Virus : This, as you can imagine is not one program, but a multitude of programs, ranging back to the late 1980s through to the present day. All operating in slightly different ways, all written using a different method, attacking machines on many different hardware platforms. A simple virus can be written with a programming skill of 75 or more. A polymorphic virus, with the capability to evade detection for several weeks on a system, may take a skill of 80 to 90, and may only be possible through using pre-written software, and collaboration with another hacker. Viruses can have many different effects, deleting hard drives, merely multiplying, crashing systems, etc. Some viruses have even been written to search for files with certain text in them, and erase them. These are slightly more sophisticated, and usually use a smaller amount of stealth to achieve their aim, as they are only likely to be active for a short amount of time, stealth is unlikely to be a major tool. These sort of viruses are more likely to be used in an espionage role, rather than basic anarchic hacking.

Chapter 6. Some handy little toys for the big boy to play with.

This can be broken down into a few subsections : Breakers, Filters, Tracers, Mappers, Killers, Blinkers, and Decrypters.

Breakers are programs designed to circumvent security programs designed to prevent access to computer systems, such as Password programs, and other security designed to prevent a user accessing specific areas of a system.

> Breakers add 30 to the target number, in effect deducting 30 from the dice roll at least on Security and Civilian rolls.
> Players with appropriately high skills in Security and Programming may modify breakers to a total of a +45 modifier, but these will crash out on a 35 per-cent chance when used.
> Breakers require a Total security skill of 60 or more, and a Programming skill of 65 or more to modify them.

Filters are programs designed to hunt specific systems for files of a particular type, or files containing keywords or specific data. This is essential to keeping the time down that you spend connected to a system.

Filters can find a file on a system only in the areas accessibly to the user, they require some search keywords, or a list of file type being searched for. These programs can be automated, to download every file they find, or simply list them when found. These programs can be run on a target system, while the hacker disconnects, so the connection is broken, and the results mailed to the user, to a false mailbox, or to any other destination of the users choosing. (on the machine being hacked ?).

If the hacker is after anything in particular, that can be identified by 3 or 4 keywords, or a standard file type, it reduces the time he has to be connected by 2 thirds, or in the case of an off-line search, he can simply run the program and disconnect, however, there is a 1 in 6 chance of this being spotted by a network admin and disconnected if it isn't a public system. Filter require a total civilian systems skill of 50 or more.

Tracers are exactly that. Programs that work backwards from the connected system, through all the GenNet nodes to track another user of a system. This could find other legit users of a system, or a hacker connecting into a system. It can also find all the nodes of a large corporate network of computers.

Tracers have to be provided with the user name being searched for, without use of a blink program, the chance of finding a user is a Networking skill of 60. If the user running the trace is not a legitimate system user, this increases to 75.
Trace rolls made by a legitimate system admin reduce in difficulty by 10 for every 15 minutes spent on a system after the trace begins.

Mappers follow the user when he travels the Net, mapping all the nodes of the Net he accesses and passes through, and provide a map of the local system when he connects to a major network. If a computer on the network if protected by any security over a -30 modifier of any subskill, it wont be able to map any computers the other side of that connection.

Mappers require no rolls to run, however, their system usage makes any connection slower, and less efficient and responsive, so extended use of them adds 5 to trace dice rolls made against the user.

Killers come in a range of forms, from Viruses, to Trojan horses, to very simple scripts. These are fairly specialised programs designed to perform a certain function, either a repeated program, or a one-shot program. A certain amount of skill is required to use these as they aren't usually available off the Net, and must be written for the specific job. Some are available however, but are usually blunt, and inefficient, and lack stealth or subtlety. These programs usually stay on the system well after the hacker has disconnected, making them a very effective tool in a variety of cases.

Some example killers :
An implanted *Trojan* horse can be inserted into any normal program used on a system, and can be set to trigger on a certain date tp delete a system, or to run a script or program.
A *sniffer* program can be set to record and store or transmit mail or file transfers made by a certain user, or any mail flowing through the system.

Killers require a Programming skill of 65 to write, for simple programs, or up to 80 for complex programs. Networking Skills of 50 plus are also required for sniffers, and any program utilising the GenNet. Security skills of 50 are required for independent programs designed to access private systems, and monitoring external systems.
Some specific hack may require a deeper range of skills to use, for instance, adding a new account to a banking system, and giving it some money to begin with, requires indexes, and

cross references to be updated. This must be planned, and a high skill in Civilian Systems may be needed to complete it without leaving traces of the modification.

Blinkers are the key to the hackers anonymity on the Net when hacking systems. Blinkers misdirect a connection through as many different nodes as possible, and are set up to shield the user from any trace on a GenNet session. They provide dead-end locations, loops, and misdirections to any trace program that attempts to locate the origin of a hackers attack. They *aren't* foolproof, but do reduce the speed with which a hacker can be tracked down.

Blinkers require a civilian skill of 60, and a networking skill of 45. Anyone with a programming skill of 75 can modify a blinker to automate functions, and reduce the skills required to use it by 10 each. This can take several hours of solid work though.
A Blinker means that any trace roll made against the user is at -30.
With an hour or so of preparation, the user can initiate a more complex route, and add more dead-end locations to use with the Blinker. With this extra preparation, the trace modifier is increased to -45. This preparation requires networking skill of 55 or more.

Decrypters are quite simple, an encrypted file can be broken into using a decrypter, to identify the method of encryption used is a programming skill of 70, and to actually decrypt it takes a security skill of 60.

Chapter 7. General Notes on Hacking

Modifying programs

Programming skills of 70 or more can be used to modify a program to make it easier to use, or to be more effective. However, the programmer requires the skills needed to use the program to be in a position to do this. A modification to make a program easier to use by a modifier of 5 means that the roll to successfully modify the program is at -5, modifier of 10 is at -10 and so on. Every modification made to a program means a 10 percent chance of it crashing when run, this is cumulative, so additional modifications may mean a 20 to 30 percent of the program failing to run. A collaboration between programmers is possible, however, both characters need the skill levels required, but any rolls required are at +10 to target.

New programs can be created, but these should provide the basic hacking tools needed by a BlackEagle cell. Any new program would normally require a Programming skill of 55 or more, with the requisite Security, Network, and Civilian computer skills relevant to the purpose of the program.

All programs used by both sides are interchangeable between each side, bearing in mind, that SysAdmin software may be mass produced and sold as such, so may cost more (or less if you pirate it, and easier to acquire) and may be as inflexible as mass produced software.

Notes on the skills required.

All of the rolls I have put in here are fairly ballpark, they haven't been playtested yet but reflect mid-level hacker characters skill levels. Feel free to fiddle where required, or when beginning level characters need to get into this. Beginner characters should go straight for GenNet distributed programs, these are primitive, but with some fairly low security systems, allow a beginner character to at least get into the basics.

The GM may want to modify rolls depending on the system being accessed, a military site, or Ma Bell's sites may have heavier security, so increase the difficulty of any rolls made when connected, security is variable, and I don't want to waste space putting in a lot of examples. Other variables may come into effect such as the location of the site being hacked, like the country that the system is in, some third world countries are badly protected due to their financial situations, so local systems may be very easy to connect to. Corporate sites, run by foreign companies however might not be so easy to crack.

Chapter 8. Some other games the hacker can play.

As I said earlier, the hacker usually has related skills that a BlackEagle cell can't do without. A hackers contacts can provide him with some handy programs and equipment.

***Smartcard**s* : most smartcards and magnetic credit cards conform to standards of usage and the way information can be stored on them. Hackers can usually get hold of and use the equipment and software to copy and/or re-program information stored on smartcards, from simply copying a card, to upping the points you have on your Shell premier points smartcard. There are many tactics and uses for these skill.

Phone systems : Many hackers are also Phone Phreakers, this is not only to avoid big bills, but using a public phone to hack from is safer than using a home location, and with the correct knowledge, can be free. Some electronics may be required, but sometimes, simply the hand eye co-ordination required to use a pair of pliers and a soldering iron is enough.

This skill is also useful in manipulating the Cellular phone system, using a phone to scan for transmissions, and listen in to those transmissions, or to clone phones so that calls can be made free of charge. As the GenNet also runs off this cellular arrangement, being able to mask GenNet addresses or fake them is a related use.

Radio LANs : Some new Local Area Networks now run using radio connection between each other and between themselves and the central computer of a network. Now, these are very short ranged, sometimes a matter of feet, sometimes up to 30-40 metres. In some cases, it may be possible to access these from outside a building, but you first need to find a valid radio frequency, and have the appropriate equipment. This takes not only some basic knowledge of radio, and the use of radio LANs, but some Network skills, and Civilian Systems skills. Say about 65 in each. However, once becoming a node in the network, a large amount of Security and System skill is required to stay in the net, and to be able to access the rest of the network, you still need to log into the network, and set up some sort of valid access.

Social Engineering : one of the oldest and most valuable, and unfortunately, sometimes the most difficult skill the hacker uses. Social engineering is the use of a social situation to extract information from someone without them realising you are only after that information, or that once they have given it away, that you put value on that information. This information can range from passwords, to methods of encryption being used/developed, locations and use of a satellite for instance, down to personal and confidential information that could be used to blackmail someone. Get a very high diplomacy skill here folks !

(note : Social engineering was the primary method for extracting information from Public relations representatives on the methods used for encrypting Sky TV's televisions signals, which led to a decryption program being written a lot sooner than if the method hadn't been known, so knowledge of cryptography isn't everything!)

There are lots of tricks and scams possible with computer skills coupled with electronics, so use your imagination.

Viruses, and scripts : Hacking isn't just about logging onto a computer and downloading information. With viruses and scripts, you can delete information regarding a certain subject, even down to deleting files that *may* refer to a job your BlackEagle cell performed, using the computer against itself is a powerful tactic. With a script file on a computer, you can make the computer do almost anything within its capabilities including mailing information, files, copying all the correspondence from a certain person using the system, with care, and calculated use of a system, a hacker can set up a user account on a corporate system, and use it as a legitimate user, possibly even without being picked up by the SysAdmin of such a system. Having a safe route into a system is like gold dust in certain areas of the Hacker Community.

The Community : Remember, you aren't the only hacker out there, and no matter how clever you think you are, there's always someone out there better than you. However, the hacker community tends towards 3 types of computer user.

The first group, normally referred to by the other two as "lamers" are the wannabes, the computer literate, who can appreciate the power of hacking, but don not have the technical knowledge to be able to do any hacking. Usually found at the fringes of the hacker community, they are occasionally good, at taking the rap for successful hacks, or for doing a little research if they think they will get any help getting into the game.

The second group are "The Elite" or 3l33t as they sometimes refer to themselves. This is actually a mixture of very, very technical hackers, sometimes very accomplished in the field, but unwilling to share any of the techniques or information citing the "if you want to learn, no-ones going to hand it to you on a plate" excuse. These hackers are very good at what they do, but will usually be completely unidentifiable, and often work for money, rather than any other commodity.

The third group are the in-betweens. Hackers with experience ranging from hacking passwords on the network at university, up to hacks on local government, or company networks. This breed are still on the way up, and can't afford to take the Elite attitude if they want to keep going *up*, so are good bets for advice, programs, and hard information, on sites they've hacked, and occasionally collaboration. This is one group that is quite capable of acting as a team with other hackers. Which brings me to my last point.

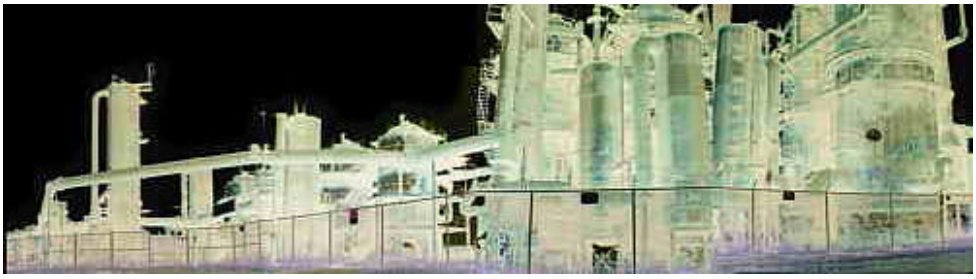
Hackers are mainly loners, the mindset has often been stereotypically described as being antisocial, but many over the past few years have devoted themselves to disproving this. As hackers have changed, so has their attitude, planned hacks can involve several hackers all attacking the same target. This increases the odds toward the hacker, a SysAdmin has a harder time responding to multiple attacks, so can be diverted from the real objective of the attack. Many of the third group of hackers are more willing to take part in this sort of exercise, to gain prestige, and respect, only occasionally (if the target is more willing to respond with physical retaliation) will money need to be offered for help.

Equipment and Prices :

Basic PC with GenNet connection :
1000 pounds Sterling
1500 Dollars
Portable Laptop with Cellular GenNet connection :
1500 pounds Sterling
2100 Dollars
Cellular re-programming software and equipment :
80 pounds
120 dollars
Basic electronic tools and materials :
80 - 100 pounds
120 - 150 dollars
Smartcard Re-programming hardware and software :
100 pounds
150 dollars
Enhanced GenNet access software (basic is free with a GenNet ready machine) :
45 pounds
60 dollars
Radio LAN hardware and software (for laptop) :
150 pounds
200 dollars
Carry case and additional Power pack for Laptop :
80 pounds
100 dollars

basic set of spares for laptop : (including hard drive, memory, power supply)
250 pounds
350 dollars
(just some ballpark figures, use and abuse)

Final Word



This is my first attempt at a sourcebook for any RPG, and I'd greatly appreciate any feedback. Mail to AleisterJCrowley@rocketmail.com. I'd love to be able to make money out of this sucker. Maybe next time eh ?

After going through this document, I have noticed some areas which need improvement, I need to flesh out a lot of the chapters with simply more information and description. I am not a hacker, but I do know a lot about the subject, having been to a few 2600 meetings, and joining mailing lists, and newsgroups on the subject. The hacker community is one of my little "hobbies", but not hacking itself.

Many of the ideas I have put into this document have come from real life. The only part of this whole thing which hasn't come from real life are a few of the programs. Taking any action against another computer hacking into your system is not an option, the most you can do is disconnect him from your system in real life, and hope to trace the hacker by negotiating with the phone companies to participate in a phone trace, over the Net, users require addresses, which are harder and harder to fake these days, so traces of these numbers is possible, but obtaining a real physical location with these can be impossible with the use of proxies, back-doors etc (if any of these words worries you never mind, if you don't understand it, it doesn't matter, that's my view anyway)

If anyone notices that the programs outlined are a little unreal, think of it this way, I have tried to standardise a lot of techniques, and obstacles, into a short list of ideas. In real life, hacking just isn't as interesting, or easy. This just puts a simpler game environment at the hands of the Milleniums End GM.

I'll update this every so often if I have any cool ideas, any ideas you want included, or any programs you think would be fun to use on the GenNet please let me know. If anyone has any graphics that'd look good in this book, let me know, and I'll put them in, if and when I can get my hands on any, I'll expand this with some system layouts, and some basic pictures. Thanks for your interest.

Thanks and Acknowledgements

Oh, and just before I go, Milleniums End is a trademark of Chameleon Eclectic games, and any terms and names that are associated with this role playing game are (so far) used without their permission, but this document (previous versions anyway) have been submitted to CE for their approval/opinion, so with any luck they won't sue me.

Thanks to the ME mailing list, and Charles Ryan for their support, and thanks to Charles Ryan and Chameleon Eclectic for writing and publishing Milleniums End.