Computers

Computers, in the form of machines that could think and store information, first became possible at TL6, but in the real world they didn't start to actually be produced until early TL7. Early computers were mostly mechanical, and it wasn't until the advent of good electronics that they really started to develop.

Computer technology is currently improving at a rate which makes it difficult to predict where things will end up.

Designer's Notes

Thinking Machines

The author subscribes to Strong AI - the belief that there is nothing magical about the human mind, and that reproducing how it works in a machine is merely a hard problem we haven't yet solved. These rules assume that true AI is possible, and any difficulties with uploading a human mind into a computer are merely engineering issues.

Computers in Yags may provide bonuses to attempts to solve problems and search for data. Computer systems between tech levels are difficult to compare, so they aren't. It is assumed that as computers get more powerful, the sort of problems they are expected to deal with get more complex as well.

Type of computer	Complexity
Micro PDA	-10
PDA	-5
Desktop (TL8)	0
Large server	+5
Mini-cluster	+10
Mainframe	+20
Data cluster	+30
NSA Super cluster	+50

Using a computer

The *Computer operation* skill covers basic use of a computer. This covers everything that is needed to be known at the current tech level in order to interface with such a machine. At TL6, it will be little more than how to load punch cards and how to interpret basic mechanical errors. Through TL7, information becomes more readily available until actual interactive use of the computer is possible, in the form of running queries and using word processors and simple programs.

By TL8, most people can be trained to use a word processor, spread sheet or to perform simple queries. By the middle of this period, *computer operation* covers advanced usage of software - such as writing macros, finding information on the internet, installing software and a little knowledge of networks and viruses.

Beyond TL8, most computer interfaces will probably be of the form of voice or mind control, making it far easier for unskilled people to control them. With the advent of true AIs, the skill may become completely redundant.

Hacking a computer

Computer hacking is the skill of doing stuff with computers - from programming to advanced networking, system design and of course breaking its security. Whilst *Computer operation* covers using programs, *hacking* covers actually understanding how they work.

Designer's Notes

Hacking Terminology

As used here, the term *hacking* refers to the term as it is used by old school hackers, originally those at MIT during the 1960s. Recently, it has come to mean 'breaking illegally into a computer system' for many people. A hacker is someone who plays with computers because they are fun, and because they want to understand how they work. Since the best way to understand a security system is to break it, hackers would often go places they shouldn't. However, once a system is cracked, most would make sure they didn't cause any damage, or let the owners know what the flaws were. Most, but not all. Many people who call themselves *hackers* however simply enjoy pushing computers to their limits, and would never break into a computer system they didn't have permission to access.

Further, not all people who break into computer systems are *Hackers*. There are some - generally known as *Script Kiddies* - who simply want to cause damage. They have little or no knowledge of how things work, but simply run scripts written by those who do.

Hacking includes programming, networking, installing and configuring. Many of these tasks are techniques which must be purchased as specialisations. For the most part, the differences between different operating systems is ignored, since this starts to get complex. If this level of detail is required, then assume that there is a *Computer hacking* skill for every type of computer system (UNIX/Linux, VMS, OS360, Microsoft etc). The same can be done with *Computer operation*.

An alternative approach is to assume a default system when the skill is first learnt, and other systems are represented by a familiarity technique, at level 2. If you aren't familiar with the system, then your roll is halved.

Computer Intrusion

Breaking into a computer system can be very easy, or very hard. Generally, getting access to information is very easy if you have physical access to the machine. At the very least, you can take it apart, pull out the hard drive (or holographic memory crystal) and make a copy to peruse at your leisure. If you don't care if the owners knew you were there, then you don't even need to make a copy.

In order to gain access to a network without having physical access, then you need to make a *Computer operation* using the *Computer Intrusion* technique. The target difficulties are given on the following table. If you don't have the right

technique, then double the difficulties. By default, an attempt takes a day.

Task	Target
Home system. Most home users know little about security, and tend to run all sorts of software which provide any number of possible security holes.	20
Small business. Small businesses may not have much more knowledge than a home user, but run fewer apps and tend to make more use of dedicated firewalls and DMZs.	40
Corporate system. Typically a large business will have a dedicated staff of IT people (or outsource such a role) who know what they are doing. Systems will be locked down, with good firewalls and restricted access.	60
Secure system. A high tech firm or important government system, where the focus is on security rather than usability. Users may be heavily restricted in what they can do, since security is seen as higher priority than productivity.	80
Military. Any system which is locked down tight, with security being the one focus of the design. Such systems are often even harder to penetrate than the difficulty would suggest, since they may not actually have access from the outside world - or at least it is restricted via dedicated lines to a few secure locations. Finding those locations will be required before any attempts are made.	100
Uptodate security Network owners have been keeping the system uptodate with the latest patches, and proactively securing the system.	+50%
Out of date The system is badly out of date, and hasn't had any patches installed.	-50%
Compromised If the system is already compromised (by trojans, viruses and the like), then it is generally easier to access.	-25%

On your first attempt to hack a system, you may if you wish make a check at twice the normal difficulty after one hour. If that fails, then a second check may be made after a day. This assumes 24 hours elapsed time, with about half that time requiring effort on the part of the intruder (the rest is running scripts, or waiting for replies on hacker's mailing lists). Further attempts may be made each day. Once you have succeeded in accessing a system, you gain a +10 bonus to all subsequent checks.

Designer's Notes

Exploits and scripts

The above table mostly abstracts the frequency of patches and updates to a system, the sort of software being run and how standard the installation is. Breaking into a home system is often easy because there are plenty of scripts available that can be used to automate the intrusion. More secure systems will have the exploits that the scripts make use of patched.

Computer systems of an earlier technology may be much easier, or much harder, to crack. If you are not prepared for the lower tech, then there is no change in difficulty, since trying to understand the long since deprecated protocols balances out any advantages gained from having better tools. If you have time to prepare however, and have access to the correct documentation and earlier toolsets, then all difficulties are halved for each drop in TL. Breaking a computer system above the TL you are used to is impossible.

If an earlier TL crosses a paradigm shift (from electronics to vacuum tubes, or AI run systems to standard programmed systems) then you also need a different skill in order to do anything with such a museum piece.

Large Networks

For many small networks, such as a typical company, once you're past the main firewall you have access to most of the rest of the system. For larger networks however, the network topology may require effort to get from the outer DMZ into more secure and/or interesting parts of the network.

For a large network then, assume it consists of multiple parts which have to be accessed separately. Assume that the first access gets you into the DMZ of the network, and from there you need to make another check to access the rest of the network.

A small company with a well designed system may have 3 sections - DMZ, standard network and financials. The latter may be a level harder to break into.

A large organisation will probably have 3-5 different parts to the network, with multi-national or central government organisations having as many as a dozen. It is up to the GM to decide what each part of the network covers.

Being detected

If pro-active monitoring of the system is being done, then there is a chance of any intrusion being noted. The sysadmin of the defending network gets a check only if they have the *System administration* technique. If they don't, then they're going to be oblivious to what is going on unless you start breaking things.

If the intruder is regularly accessing the system then the sysadmin gets to make a *Intelligence x Computer operation* check against a difficulty of 20 each week. If they have the *Computer security* technique, then this check is made each time the intruder accesses the system, or at least each day. For every level of success that the intruder got when breaking into the system, add +10 to the detection difficulty.

It is unlikely that the system is being monitored constantly - unusual logins may be noted in logs several hours after you've grabbed what you wanted and disconnected. This can provide you with time to try and cover your tracks. Futuristic systems monitored by AIs may have an instant response however.

It's Too Hard

Often, a system will be too secure to gain access to, so it will be necessary to find less direct ways of getting into the system. Each option can only give you a single bonus (so digging through lots of rubbish on multiple nights only gives you the best bonus), but different options can stack together.

Designer's Notes

Feeling Lucky?

Luck plays an important factor in a lot of these cases, mostly because a lot of it really will come down to luck. It doesn't matter how good you are at looking through rubbish, if the company hasn't actually thrown out anything useful.

Skill can help still of course, since it both helps to identify useful things, and is also needed to put it to use. However, many of these risky tasks can be carried out by people who don't know much about computers.

Just Steal It

In any modern setting, many employees of an organisation will work from home, or at least have a way of accessing the main network whilst away from the office. If this is the case, then obtaining access to their laptop, home computer or PDA can provide a large advantage. Obviously, this requires some basic theft, or at least house breaking.

Gaining access to an external point of entry will drop the difficulty by one or two levels (e.g., from *Secure* to *Corporate* or *Small Business*). Non-technical employees often make the best targets, especially if they've simply installed VPN software on their home computer. It may be possible to break into their home PC remotely, then install key loggers or trojans to help provide you access.

Dumpster Diving

People through away all sorts of useful stuff, and digging through their waste may show up notes containing passwords or internal network diagrams that provide you with something useful.

Each night of searching, make a *Luck* check. On a 20+, you'll find something possibly useful. The GM makes a second *Luck* check for you to determine how useful it is, but you won't know what bonus (if any) it provides until you try to make use of it by another intrusion attempt.

What you find...	Luck Roll
Information is out of date, or wrong, and provides no bonus.	< 10
Some information about their network topology which gives a +5 bonus.	10+
List of public facing applications or firewall configuration, +10 bonus.	15+
Some useful passwords or information about possible security holes, +15 bonus.	20+
Looks like someone has chucked out their secure id token, +25 bonus.	25+

You gain a +2 bonus to both *Luck* checks if you have the *Dumpster diving* technique. The usefulness of the information fades over time, so reduce the bonus by +5 each week. Multiple bonuses don't stack. Note that anyone can search through rubbish, but if you don't have the *System administration* technique, you have a -2 penalty to the first Luck check.

If the organisation makes an effort to destroy information before throwing it out, you have a -10 to the second check. If they have good processes in place, then it becomes almost impossible to find anything, and you suffer -20. Remember, a secure building may also have guards in place to stop this sort of thing as well.

Down the Pub

People like to go down the pub at lunch time (or after work) and often talk about their job. If you can locate the network administrators and listen in on their conversations, then you might hear something useful.

Each day, make a *Luck* check as for *Dumpster Diving*. If you don't have at least *System administration*, then there is a -5 penalty to the second check, and -2 if you don't have *Computer intrusion*. It really helps to understand what they're talking about to make use of the information.

If you're feeling really sociable, then you can try to join them. Make an *Empathy x Charm* check at 20+ to be able to join them without them clamming up. Assuming that they're a group of young males, then being a young good looking female geek who appears interested in technical stuff can really help.

Once you've joined them, then you gain an automatic +1 to the first *Luck* check, plus a further +2 for each extra level of success. Double these if you have either the *Carousing* or *Flirt* techniques (the latter only if suitable), or triple if you have both.

You have the option to try and prod them into giving you information by making both a *Empathy x Guile* check, and an *Intelligence x Computer operation* check at one of the following difficulties (your choice). If you fail,it means that they get suspicious about you. If you have *Carousing* then you can avoid suspicion by a second guile check (same difficulty), but you won't be able to try again.

Bluntness	Target
Subtle questions to prompt them, can give a +1 Luck bonus.	20
Less subtle questioning, but gives a +2 bonus.	30
Quite directed questioning which would be obvious if they thought they were with customers or competitors. +3 bonus.	40
Blunt and direct questions which you can only get away with because you're so nice, +4 bonus.	50

The *Luck* bonus in this case applies to both Luck checks (and stacks with the bonus from the first roll for the first Luck check). If you have *Carousing*, you can double this second bonus.

If they are paranoid for some reason, there is a +50% increase to all Empathy related checks, or +100% if they are actively alert. Note that some organisations have their own pubs inside the building specifically to stop this sort of thing from happening.

Social Engineering

Often, the easiest way to get information out of a secure network, is to simply ask for it. People have a tendancy to be helpful, and can be persuaded to give away information they shouldn't when they see someone having trouble.

The normal technique is to either phone up an organisation, or visit the front desk, and ask some leading questions. For example, you could contact the IT help desk with a technical query (pretend to be an employee, and claim that your VPN isn't working), or turn up at the offices for a fake meeting.

Make a *Will x Guile* check on the previous Bluntness table. If you have *Cold reading*, you can double any Luck bonus you receive.

Encryption

Secure computer systems will ensure that data is stored in an encrypted form. Generally, anyone with access to tools and knowledge of a later TL, is able to crack the encryption of an earlier TL without much effort. Divide the difficulty by 5 for each difference in TL.

The exception will be data properly encrypted with a one time pad - such data is generally perfectly safe unless access to the pad is possible, or a mistake has been made. One time pads are difficult to manufacture for large amounts of data however, so such encryption is rare.

An attempt to break modern encryption can be made using *Computer hacking*. Most such attempts involve brute force techniques, using software to do most of the work. If you have the *Encryption* technique, you can halve the difficulties.

Task	Target
Very basic encryption. A custom encryption system for a proprietry system, written by someone with no cryptographic background. Many programs may store passwords or license keys in this form.	20
Standard encryption. The sort used by common off the shelf encryption software, assuming that no major effort has been made to keep it secure.	100
Secure encryption. The best commonly available encryption. This is often used for financial data or security tools.	150
Military encryption. The very best levels of encryption, where cost (in time, effort and computing power) is no limit when securing data. The military will rarely use this level of encryption, especially for real time communications, since it is too expensive unless there is a dedicated mainframe at each end.	200

The standard time to break the encryption on a document is 100 days for a desktop of the equivalent TL. If a more powerful, or less powerful, computer system is available then add the computer system's rating to the attempt. Each level of success above the required difficult reduces the time required by 90% (e.g., 10 days for a good success, 1 day for excellent etc).

If a more random approach is desired, then assume that the base time is d20 x 10 days. This makes it harder for a player to know how long it's going to take. As with intrusion, it is assumed that about half the time is waiting for scripts to complete, and half the time requires the cryptographer to be working on the problem.

Designer's Notes

Breaking encryption

Breaking encryption can be hard, and often it can only be done by either brute force, or finding a mistake in the process. Here, it is assumed that most of the work is in trying to exploit flaws in the implementations rather than trying to break the mathematics behind the algorithm.

Generally, any real encryption system is designed so that brute force methods take longer than any reasonable time to work.

If you have *Cryptography*, then you can attempt to find a shortcut to reduce the amount of computer time required. How difficult this is depends on the amount of data available, whether there are known flaws in the encryption system used, or if common mistakes have been made. Each type of shortcut can be attempted, and each level of success means that the decryption difficulty is reduced by 10 (minimum 10).

Task	Target
Known flaws. If the encryption system has some known flaws, then it may be possible to exploit these. Will tend to apply to older software.	20
Type of data is known. If the type of data being encrypted is known, then this information can be used to decrypt it. For example, if the data is a document in a common word processor format, which always has the same header information, then this can be used to help crack the protection. The cracking of the German Enigma system in WWII was helped by German weather reports always starting with the same text.	30
Large amount of data. If there is a large amount of similar data, then this can help find patterns, and lead to a shortcut.	30

All attempts stack, so if there is a large amount of data and known plain text, then it can be very easy to decrypt documents. Note that the above attempts can only be made if they are applicable.

Artificial Intelligence

AIs are self-aware intelligences implemented as software. There are a number of different types of AIs, and they range considerably in their capabilities.

Turing Personality

A *Turing Personality* is simply a software program that is able to convince people that it is human. It does not have full consciousness however, and is only capable of operating in a narrow field. They are often used on support desks or in service roles such as shop assistants or performing basic servant duties. Outside of their realm of expertise, then rapidly lose competence, and have only limited learning capability.

TPs become available around Tech Level 9, and by TL 10 may be commonly available as the interface to PDAs or specialist software programs.

Virtuals

Full virtual personalities are available from TL10 (or higher, depending on the background). These are fully conscious

and self-aware entities, who have all the capabilities of a human mind. At the TL that they are introduced, they are about as capable as a human, but with better recall and data retrieval. Working out answers to 'tricky' problems takes about as much time as a human does. They are assumed to run on a mainframe class of machine.

Each extra TL beyond introduction, assume that they can run on a machine of one lower class with about the same level of ability, or they can run about 10 times as quickly on the same level of hardware.

Mind Interfaces

Basic mind-machine interfaces become available at TL8, though it isn't until TL9 that they really start to become useful. Basic PDA functionality can be accessed (map, contact or appointment information overlayed onto the optic nerve), and it becomes possible for a mind interface to be used to operate a computer (in much the same way a keyboard or mouse is at TL8).

At late TL9, early TL10, it is possible to record everything that a person sees.

At TL10, it becomes possible to access enough information to allow full body immersion into virtual realities, with sound and images from surface thoughts being accessable to the machine.

At TL11, it is possible to read some memories out of a mind, and writing is possible but flaky. The main issue is accessing the memories, since they need to be brought to the fore and read. Every mind is different, so a large amount of time must be spent adapting to an individual before there is any hope of searching memories. Trawling memories is slow, and is effectively limited to real time. Even then, false memory syndrome is a very real possibility.

By TL12 a lot of the adaption problems have been sorted, but downloading a person's mind is slow and difficult. Brain taping is possible, but it is traumatic, and can result in lost or damaged memories. It can take about a month to fully brain tape someone.

Cyberware

Most cyberware is limited to providing physical enhancements to a person - making them faster and stronger for example. Enhancements to senses tend also to be limited to doing what they say on the box and no more. As soon as cyberware is available it is possible to network such addons to each other and to external interfaces, but doing so is a security risk which most people aren't willing to take. The possible law suits that could result if someone is damage due to a cyberlimb contracting a virus means most companies are unwilling to sell them with any form of connectivity.

As TL9 progresses, sensory devices begin to be able to store and forward data, increasing the advantages of linking them up with external interfaces. Some will require a wired interface, and tend to be secure. Those that have wireless interfaces are less secure and can be hacked as if they were a *Secure system*.