by Christian Conkle

A Fuzion Plug-In

by Christian Conkle
(conkle@europa.com, http://www.europa.com/~conkle)

Introduction

This is a system of rules expanding the hacking rules for Fuzion and Interlock. These rules draw heavily on Cyberpunk 2020's Netrunning rules and are intended to be native in a Cyberpunk environment where neural cyber-interfaces are standard, though they are written generically enough to be useable in a modern setting as well.

These rules were designed to use existing Cyberpunk 2020 equipment and software with little modification. There are several differences from the original rules, however, that are intended to speed play and optimize simplicity. First, these rules lack a grid. Movement within the virtual environment of cyberspace is conceptual. To convert applications that give "ranges", simply apply a percentage chance of effectiveness based on range. Second, these rules incorporate the Power attribute from other Fuzion games, essentially the equivalent to a computer's Intelligence from CP2020. Third, software and memory no longer needs to be assigned to specific CPUs. If the GM wishes, each MU of application and datafile can be assigned to specific CPUs such that if that CPU fails, the application or datafile is no longer available. This process was removed to eliminate extra bookkeeping.

These rules assume a 3d6 die-rolling mechanic option of Fuzion. If you're playing Interlock, or the Fuzion option of 1d10, simply replace the 3d6 with a 1d10 die roll. You won't achieve the same kind of bell curve, but the results will be sufficiently randomized.

The Net

The Net is a global computer network allowing fast and convenient access to millions of computers from any other computer on earth or beyond. Any computer connected to this network has the capability to access information from any other computer connected to this network regardless of distance or time of day. Whether it is called the Internet, the Web, the Cybernet, the Face, or the Net, all use different special effects and technologies to describe the same thing. This plug-in assumes a near-future setting which makes use of a Virtual Reality interface and gives exciting names to actions and tasks which can be easily modified to fit a more mundane modern setting.

All computers connected to the Net are assigned LDL. This LDL serves as a kind of telephone number for that computer, to which other computers know where to send information. In a futuristic setting, a Virtual Construct or Icon may substitute for the LDL. The Net User connects their computer to a Virtual Reality Interface, within which companies pay for space and create elaborate virtual constructs to represent their LDL, the VR equivalent of Internet Portal Sites such as Infoseek or Yahoo! today. The Net User may now tour the bustling 3D Virtual City regardless of gravity or speed. Corporate virtual constructs are like giant 3D advertisements, attempting to entice the average Net User into their Virtual Realities to sell products or services. Some Virtual Realities actually provide useful services such as information or online software applications. The VR equivalent to modern Web-sites.

These Virtual Realities are housed on Dataservers maintained by the respective corporations or institutions. It is the information housed on these Dataservers that isn't readily available to the public that draws the Hacker.

Normally, a corporate dataserver is openly accessible to the Net public, providing information either to the public or its employees through a variety of interfaces: text-only, text and graphics (the Web), audio/video, or full-sensory virtual reality (the Net).

However, the value of information available on public dataserver sites is poor and bland. In addition, access to remote software applications is limited to public-domain applications.

Instant Netrunning

by Christian Conkle

Datafortresses are the restricted hidden levels of a dataserver providing remote access to restricted data or software applciations to authorized users. Security is maintained through the datafortress' DataWall program. The level of security restriction depends on the value of the information or application. Secure information may be housed on the same dataserver as public information, only hidden in restricted directories, effectively invisible from those who lack proper authorization. Authorization comes with proper identification.

Identification can come in many forms: Authorized Net LDLs, passwords, proper interface software, or even biometric data.

It is a hacker's goal in life to gain unrestricted access to restricted information, uncover secrets, make unauthorized changes to data, or to use a restricted software application.

When attempting to gain unauthorized access to a corporate datafortress, the hacker establishes a legal connection to the company's dataserver. Once connected, the hacker has normal access to the free services. Normally, an authorized user will then use an interface program to gain access to the datafortress. The datafortress' Code Gate program verifies authorization and allows access. The hacker attempts to fool the code gate into authorizing entry. Should that fail, the hacker may attempt to gain entry by disabling the DataWall program protecting the information.

Once past security, the Datafortress constantly re-checks authorization through the use of Detection software. Detection software double-checks the authorization of all the users connected to the datafortress. If it finds a discrepancy or error, it notifies the Datafortress System Administrator (SysAdmin) who will either attempt to disconnect the hacker, determine the hacker's location with a Trace application, disable the hacker's software with an Anti-ICE application, disable the hacker's computer with Anti-System software, or physically injure the hacker with Anti-Personnel software. The hacker uses Stealth software to fool detection software into either authorizing or ignoring the hacker's connection. If discovered, the hacker may fight back against the SysAdmin with Anti-ICE, Anti-System, or Anti-Personnel software of their own.

Should the hacker gain access to the Datafortress' directories, they may view, copy, or alter data. Data comes in the form of online applications for remote use, inter-office communication, public display data (text, audio-video, or VR), databases, or records.

The Hacker

The Hacker's arsenal includes a computer, specialized hacking software, and, foremost, a way to connect to a remote target computer, usually via the Net though direct connections, however unwise, can be made.

A Hacker's access to the Net is very important. To connect to the Net, the Hacker must have an LDL. LDL's cost 50 euro a month from the Internet Corporation, though they, too, can be hacked. Connections between computers are relatively easy to trace. Each computer connection has a corresponding Trace Value from 1 to 10. Hackers generally make a chain of several connections before they proceed to their target computer. A SysAdmin wishing to trace the ultimate origin of the Hacker must trace every connection to find the source.

The SysAdmin

The SysAdmin is in charge of security for a Dataserver/Datafortress. It is their primary job to prevent Hackers from illegally gaining unauthorized access to restricted data. It is their secondary job to catch hackers who have already have.

SysAdmins use their own computers connected to a Dataserver/Datafortress to execute software applications. The Dataserver/Datafortress itself uses software such as Codegates, Datawalls, and Detection software deter and identify hackers, yet allow authorized users in.

A Datafortress is also characterized by its Power and its Speed. A Datafortress is also rated by a Security Level from 1 to 10. This number is added as a skill would to the computer's Power when executing software applications. The computer's Security Level is also it's Trace Value if being used to chain connections.

A SysAdmin can't do anything to catch a Hacker if he doesn't know they're there, so the SysAdmin relies heavily on Detection software to notify them of unauthorized access. Once detected, the SysAdmin can run Anti-Personnel software against the intruder, or opt to trace the hacker and run Anti-System software against the Hacker's computer.

The Computers

Computers, whether they are Palmtops, Desktops, Minis, or mainframe supercomputers, exist to execute software applications. The computer is characterized by its Power and its Speed and its Security Level.

The Power is used like the computer's Body and it's Reflexes, it determines it's resiliency to attack and its base chance to perform an action. Power is based on the number of Central Processing Units driving a computer. One CPU has a Power of 3, each additional CPU adds an additional 3. Each CPU costs $10,000. A Computer may have up to 7 CPUs for a Power of 21. Additional CPUs increase processing capacity and provide backups in case one CPU should fail due to Anti-System software.

A Computer's CPU also determines how much software it can run and data it can store. Software and Data are stored in Memory Units. A Computer can store as many MU's as it's CPU x 40. Memory can be improved for $250 per MU. CPUs also determines the starting level of system Datawall. A Datafortress' base Datawall strength is equal to the number of CPUs driving it. Computers with Powers higher than 10 are Artificial Intelligences with complete personalities and full interactivity. Power can be decreased for a cost reduction of $3000 per level.

A Computer may also possess skills like a character. Memory can be put aside to use as skills at a rate of 1 MU per Skill Level. In this way, a computer can devote 5 MU to have a Security Skill of 5. All computer skills use Power as the primary statistic.

The Speed is used to determine initiative. If using the Speed Chart, it can be used to determine the number and order of actions in a turn. Speed can be increased for $2000 per bonus up to +5.

The Security Level is the SysAdmin's Security skill, added to its Power when resisting attacks. The Security Level is also used to determine a server's Trace Value when using it to chain connections in preparation for a run.

A Computer can respond to hacker's automatically. Once Detection software has identified an unauthorized intruder, the Computer can automatically execute Anti-Personnel software against the Hacker, or trace the signal and run Anti-System software against the Hacker's computer.

A Computer can also be defined as a Cyberdeck. Cyberdecks or Cybermodems are small devices that are similar to computers in that they execute programs, but are different in that they are connected to the user's living brain and use it's neurological wiring to act as its Central Processing Unit. The Cyberdeck, modern terms, is little more than a hard drive and network connection. All input and output is processed by the user's brain.

Cyberdecks do not have CPUs, but the user must have a Neural Interface and Cybermodem processor installed in their brain, the cost of which is $1100 for the hardware and $500 for the surgery. Cyberdecks provide 10 MU, a Speed of 0, and have a Data Wall strength of 2. The basic parts of a cyberdeck costs $1000 for the external hardware, though this is often marked down to as low as $500 for a used model.

by Christian Conkle

Computer Hardware Price List

1 CPU	$10,000 (Power 3, 40 MU, Data Wall Strength of 1)
1 Cyberdeck	$1000 (Power 0, 10 MU, Data Wall Strength of 2)
+1 CPU	$10,000 (Power +3 each, +40 MU each, Data Wall Strength of +1 each, maximum 7 CPUs)
+1 MU	$250 (no maximum)
+1 Speed	$2,000 (maximum of +5)
-1 Power	-$3,000 (no maximum, but at more than -2 you may as well buy fewer CPUs)

Cyberdecks vs. Computers

In games where cybernetic interfaces are common and older manual interfaces are uncommon, simply apply a -2 to all actions taken by manual-interface computers. In games where cybernetic interfaces are uncommon, such as the modern world, apply a +2 to all actions taken by cybernetic interface computers.

Successful attacks made against Cyberdecks using Anti-System software will cause the brain to disconnect and become unconscious for 1d6 rounds in lieu of the CPU.

The Menu

To simplify using a computer in a game context, a simple set of commands has been devised. These commands are called “The Menu”. A Hacker simply chooses his action based on the list available in the Menu.

The Menu

Log On/Off: Legally gain access to an unrestricted Dataserver through proper authorization techniques (password, LDL authentication, or biometrics).
Run Program: Run either a local or remote software application.
Read File: View the contents of a datafile, be it Text, Graphics, Audio/Video, or Virtual Reality.
Copy File: Copy a file from a remote location to a local one. Warning, a record is kept of each copy in a file history.
Edit File: Edit the contents of a datafile above. Warning, a record is kept of each modification in a file history, including the modification of the file history.
Erase File: Erase a datafile above. Warning, a record is kept of each erasure in a file history, including the erasure of the file history.
LDL: Establish a connection to a Dataserver. Warning, if disconnecting from datafortress, if the stealth roll was unsuccessful, the SysAdmin can still do a trace on your LDL.

Instant Netrunning

by Christian Conkle

The Software

Software applications are measured by their Strength, which act as a sort of Weapon Accuracy which is added to all tasks performed with that application. Software Strength is rated from 1 to 10.

Software is also measured by how many Memory Units it uses on its host computer. This is cumulative. A computer with 30 Memory Units can run one 15MU program and three 5MU programs simultaneously. Switching out a program takes one action.

Software applications can have very specific effects, depending on the application being used. The most common and broadly-defined applications are as follows:

Type	Effect	Strength	MU	Cost
Decryption (Wizard's Book)	Defeats Codegates and File Locks.	4	2	400
Intrustion (Hammer)	Defeats Datawalls.	4	1	400
Stealth (Invisibility)	Defeats Detection Software.	3	1	300
Protection (Shield)	Defeats Anti-Personnel Software.	3	1	150
Anti-System (Flatline)	Causes system to crash.	3	2	570
Anti-ICE (Killer II)	Does 1d6 damage to target software's STR.	2	5	1320
Anti-Personnel (Hellbolt)	Does 1d10 Hits directly to target's body if connected via a cyber-jack.	4	4	6750
Firewall (Datawall)	Prevents all access to restricted information.	POW +1	- +1	- +1000
Authentication (Codegate)	Allows access to restricted information to authorized users	2 +1	1 +1	2000 +1000
Detection (Guard Dog)	Detects unauthorized users, traces signal, and alerts SysAdmin.	4	5	720

Other software found in Cyberpunk 2020 is fully compatible with this system.

Utilities

Utilities are programs that help the Hacker in between runs. Though most don't provide any practical application during the run, they're nonetheless essential applications for the upkeep and preparation of a hacker's computer.

Restore Utility (ReRezz)	Recompiles and restores destroyed programs.	3	1	130
Recorder Utility (Instant Replay)	Records activities of current Hack for replay later.	8	2	180
Virus Protection Utility (Gatemaster)	Detects and destroys Virus programs.	5	1	150
File Protection Utility (Electrolock)	Locks datafiles as a Strength 3 Code Gate.	7	2	170
Compression Utility (Packer)	Reduces program size by 1/2. Takes 2 turns to unpack.	4	1	140
Backup Utility (Backup)	Creates copies of most programs on chip.	4	1	140
VR Map Utility (Cartographer)	Supplies complete system map of VR interface.	6	3	200
Utility Package	All of the above in one package. Saves MU and money.	5	10	1000

by Christian Conkle

Standard Hacker Software

Decryption (Strength 4, MU 2, $400)
Intrusion (Strength 4, MU 1, $400)
Stealth (Strength 3, MU 1, $300)
Protection (Strength 3, MU 1, $150)
Anti-ICE (Strength 2, MU 5, $1320)
Total (MU 10, $2570)

Standard Datafortress Software

1 - **Mundane Systems**
Detection (Strength 4, MU 5, $720)
Total (MU5, $720)

2 - **Grey Systems**
Detection (Strength 4, MU 5, $720)
Anti-System (Strength 3, MU 2, $570) Grey Systems Only
Total (MU 7, $1290)

3 - **Black Systems**
Detection (Strength 4, MU 5, $720)
Anti-System (Strength 3, MU 2, $570) Grey Systems Only
Anti-Personnel (Strength 4, MU 4, $6750) Black Systems Only
Total (MU 11, $8040)

Sample Computers

1 - **Minor business** or **personal system** (grey info)
Statistics: POW 1 (1 CPU, -2 POW) , MU 40, Speed 0, $4000
Example: DataTerms, Minor Personal Information, Palmtops, Portable Computers.

2 - **Major business** (grey info) or **personal system** (black info)
Statistics: POW 3 (1 CPU), MU 40, Speed 3, $16,000
Example: Business Accounts, Secret Personal Information

3 - **Major business** (black info) or **Megacorp system** (grey info)
Statistics: POW 6 (2 CPU), MU 80, Speed 6, $32,000
Example: Alternative Accounts, Customer Sales Information

4 - **Government** (grey info), **Megacorp** (black info) or **Criminal system** (grey info)
Statistics: POW 9 (3 CPU), MU 120, Speed 9, $48,000
Example: Police Files, Sabotage Information, Holdings Information

5 - **Government** (black info), **Orbital** (grey info), or **Criminal system** (black info)
Statistics: POW 10 (4 CPU, -2 POW), MU 160, Speed 10, $54,000
Example: Black Op Files, Internet Account Holders, Face Bank Accounts

6 - **Orbital system** (black info)
Statistics: POW 12 (4 CPU), MU 160, Speed 12, $64,000
Example: Agora Mecca, Cyber Circle Lunar, Ishima Orbital Databases, Artificial Intelligences.

by Christian Conkle

The Goods

Once a successful Hacker has bypassed security (Datawalls, Codegates, and Detection software), he now has access to the Datafortress' CPU. The Hacker may now view stored files (text, video, audio, VR) or run online software applications. Be warned, individual files may have further security measures attached to them. For example, a file marked "Black Ops: Top Secret" might have another Detection application attached to it which the Hacker must bypass. Or it may be file-locked. Tampering with any ICE applications automatically requires the Hacker bypass a File Protection Utility and any Detection Software.

Common datafiles found on corporate datafortresses include:

1 Inter-Office Memos (E-Mail)
2 Promotional Material(such as VR advertising sims and Web Pages)
3 Business Records (including databases)
4 Financial Transactions
5 Grey Ops
6 Black Ops

CPU's house applications for online use as well. Applications range from simple spreadsheets and word processors to VR Simulations and computer-controlled robotic systems such as security video surveillance, elevators, building climate-control, assembly robots, etc.

Note on making copies: In the Cyberpunk future, all files have a file-history, recording all modifications to the file. Though modifications can be made to the file-history, the File-history now has a record of the modification. This feature is used to determine the propriety of data. For instance, a hacker finds a file in the Arasaka database called "Black Ops: Top Secret". The File History for that file will indicate how many times it's been viewed, by what User, and when. Our Hacker decides to make a copy. The original now records that a copy was made at this date by this user. The new Copy records that it was copied from an original on this date by this user. Every time the hacker views the material, the record shows that the file was viewed on this date by this user. If the hacker wishes to sell this information, a prospective buyer can view the file-history and see how many times the file has been seen, modified, and copied and by whom. Diluted data will lower the file's value. Virgin data will raise it's value. The enterprising Hacker can easily change the File-History, but a record is made that the file-history has been changed, thus lowering the value even more. The Hacker can then try to delete the record of the change, but the deletion of the change is recorded in the file-history. It never ends. The safest bet is to just own one copy and not view it.

by Christian Conkle

Steps in Cracking a Datafortress:

1. Library Research (*Intelligence + Library Research + 3d6 vs. Diffiuclty Number*) to determine little facts about the corporation. The margin of success is granted as a bonus to the Decryption roll in step 2.

1a. The Hacker loads up a good selection of software. Necessary applications include one Decryption, one Intrusion, one Stealth, one Anti-ICE, and one Protection.

2. LDL(*Roll over LDL Security Level on 1d10*). The Hacker has connected to a remote server and may use it to connect (LDL) to another remote server, making a chain of connections to their target. SysAdmins must trace each connection to determine the Hacker's LDL. Once a chain of connections has been established, the Hacker may use the same chain indefinitely unless access is revoked by the remote server's Net Access Provider.

If unsuccessful, the remote server has refused to connect the Hacker. The Hacker must then make a final connection to the target server.

3. Decryption vs. Codegate (*Intelligence + Hacking + Decryption Program Str + 3d6 vs. Power + Security + Codegate Str + 3d6*). If successful, the Hacker has fooled the Code Gate into allowing unauthorized access to the server. The Hacker is still susceptible to Detection software, proceed to step 4.

If unsuccessful, the Hacker still has no access to the server. Repeated failed attempts(3d6) will cause any Detection Software to alert the SysAdmin to the attempt who may use Detection software to initiate a trace to locate and/or monitor the possible Hacker. Continue to Step 4.

4. Intrusion vs. Datawall (*Intelligence + Hacking + Intrusion Program Str + 3d6 vs. Power + Security + Datawall Str + 3d6*). If successful, the Datawall has been circumvented and the hacker now has access to the server. The Hacker is still susceptible to Detection software, however. Proceed to step 5.

If unsuccessful The Hacker still has no access to the server but may have been noticed. If unnoticed, try again. If noticed, either a SysAdmin or an Anti-Personnel Program has been notified of the Hacker's presence and will attempt to apprehend or discourage him, proceed to Combat!

5. Stealth vs. Detection (*Power + Security + Detection Str + 3d6 vs. Intelligence + Hacking + Stealth Str + 3d6*). If successful, the Detection Software has detected no unauthorized activity but may attempt to re-validate the user after an interval of time (3d6 rounds), proceed to step 6.

If unsuccessful, the Detection Program has detected unauthorized activity and may notified either a SysAdmin or an Anti-Personnel Program to apprehend or discourage the Hacker, proceed to Combat!

6. You now have access to the CPU. The computer thinks you are logged on as an official authorized user. You may access datafiles and software applications available on that server. Some datafiles and applications may contain further security measures. If so, repeat step 3.

7. Cover your tracks. Failing to log off or being cut from the line means that the SysAdmin can still trace your location. Be sure to always log off properly. View the contents of any file you download, but be wary of the file-history: don't dilute your data!

by Christian Conkle

Combat!

1. Initiative.
Human Intelligence + Computer's Speed + 3d6
Computer's Power + Speed + 3d6

2. Loser declares first, Winner acts first. Therefore, if the loser is launching an Anti-Personnel Program towards the intruder, the winner may either activate a suitable defense or take a chance and attack the loser first.

3. Combat Options:

3a. Intruder attacks ICE. (*Intelligence + Hacking + Anti-ICE Program Str + 3d6 vs. Computer's Power + Security + Program Str + 3d6*). If successful, the target software application has crashed and erased from the server.

If unsuccessful, the attack has failed to crash the application. Detection Software automatically traces the Hacker's connection and alerts the SysAdmin to the attempt who may attempt to discourage the Hacker.

3b. Intruder attacks SysAdmin or SysAdmin attacks Intruder. (*Intelligence + Hacking/Security + Anti-Personnel Program Str + 3d6 vs. Protection Program Str + Intelligence + Hacking/Security + 3d6*) If successful, the Anti-Personnel program has done damage directly to the user's brain (STR - Protection STR in Hits), only if connected via a cyber-modem. On older non-cyber connections, treat attack as an Anti-System attack.

If unsuccessful, the attack has failed to do any damage.

3c. Defending CPU attacks Intruder
(Computer's Power + Security + Anti-Personnel Program Str + 3d6 vs. Intelligence + Hacking + Protection Program Str + 3d6) If successful, the Anti-Personnel program has done damage directly to the user's brain (STR - Protection STR in Hits), only if connected via a cyber-modem. On older non-cyber connections, treat attack as an Anti-System attack.

If unsuccessful, the attack has failed to do any damage.

3d. Intruder attacks System. (*Intelligence + Hacking + Program Str + 3d6 vs. Computer's Power + Security + DataWall Str + 3d6*) If successful, the Anti-system software has caused a CPU to crash, ceasing all activity until the CPU can be re-initialized using a Restore Utility. The Intruder is immediately disconnected, but not logged off. Once the CPU is re-initialized, the SysAdmin may attempt the trace the connection. If the target is using more than 1 CPU, all CPUs must be neutralized for the target to crash.

If unsuccessful, the attack against the CPU failed. Detection Software automatically alerts the SysAdmin to the attempt who may initiate a trace to locate and/or monitor the possible Hacker.

3e. Detection Software Traces Intruder (*Power + Security + Program Str + 3d6 vs. Intelligence + Hacking + Trace Value + 3d6*) If successful, the Detection Software has located the origin of the Hacker's connection and informed the SysAdmin. A Detection Program must trace each connection in the event of chained connections (see above) to determine the origin. Once determined, the SysAdmin may notify the Hacker's Net Access Provider in an attempt to have their access revoked. In addition, any further attempts to connect from any server on a traced chain will automatically alert the SysAdmin's Detection Software of the unauthorized access. If a connection was severed without spending an action Logging Off, the SysAdmin can still perform a Trace on that severed connection.

If unsuccessful, the trace has failed. The Detection Program may attempt to trace a connection each round.

3. Damage. Damage is allocated to affected systems or programs (or Hits in the case of Black ICE).

by Christian Conkle

Glossary

Anti-ICE Software: software meant to crash and delete other software applications.

Anti-Personnel Software: software meant to do damage to the actual Netuser. Only works in mileu that use Cybernetic interfaces.

Anti-System Software: software meant to crash or immobilize another computer's CPU.

Artificial Intelligence: an advanced computer capable of full interaction and decision-making.

Black Info/System: Top Secret information. Information that someone is willing to kill to keep secret. A Datafortress with deadly countermeasures such as Anti-Personnel software.

Codegate: a Cyberpunk 2020 term for an authentication mechanism or Firewall. Codegates could check name-password combinations, computer location (LDL), fingerprints, retinas, voice-prints, DNA, etc.

CPU: Central Processing Unit, the brain of a computer. Many computers have multiple redundant CPUs that increase processing power. Also, if one fails, the computer can keep operating at a reduced level.

Cyberdeck: or Cybermodem, a computer device that uses the operator's living brain as a CPU.

Datafile: any file that contains information. Datafiles can be text, graphics, video, audio, or full sensory VR simulations.

Datafortress: A Dataserver that restricts information to authorized users.

Dataserver: A futuristic term for a server, a computer which provides data upon request.

Datawall: A Cyberpunk 2020 term for a Firewall, a Datawall without a Codegate simply doesn't provide access to it's protected information and must be defeated with Intrustion Software.

Decryption Software: Software designed to bypass Codegates by fooling it into providing access.

Detection Software: Software that periodically re-checks users on a server to authenticate access. If unauthorized access is discovered, the Detection Software notifies the SysAdmin or automatically deploys Anti-Personnel or Anti-System applications depending on how the Datafortress is set up.

Euro: The Cyberpunk 2020 unit of currency. For modern settings, simply replace with dollars.

Grey Info/System: Secret information. Information no one is willing to kill to keep secret. A Datafortress with non-lethal countermeasures such as Anti-System software.

Hacker: A generic term for anyone attempting to gain unauthorized access to restricted information of applications.

Hacking: Skill used by Hackers. In game terms, Hacking and Security are the same skill used for different purposes.

ICE: Intrusion Countermeasure Electronics, encompassing any software applications designed to prevent unauthorized access to a Datafortress.

Icon: A visual representation. In Cyberpunk 2020, refers to a 3D representation of a computer object. A file might be represented by an icon that, once clicked/grabbed/pushed/opened, will display the contents of that file. Often, events are represented by an icon. For instance, a SysAdmin might represent his presence on the server with an icon of a knight in armor. If the Hacker sees a knight in armor, then he knows the SysAdmin is logged onto the server.

Internet Corporation: A Cyberpunk 2020 creation meant to be a conglomerate of Net Access Providers. In the modern world, these would be comprised of several companies such as MCI, ATT, UUNet, etc.

Intrusion Software: Software meant to temporarily disable Datawalls, allowing access to the server. The disadvantage is that their use may alert Detection Software applications.

by Christian Conkle

LDL: A Cyberpunk 2020 equivalent of the modern IP address. In Cyberpunk 2020, the LDL also serves as an all-purpose phone number, e-mail address, and voice-mail box.

Memory Unit: A Cyberpunk 2020 equivalent to Megabytes. It has no real-world conversion and was used in lieu of actual future memory sizes which can become dated quickly.

Mundane Info/System: Confidential information, but hardly a secret. Information that is restricted but isn't guarded by countermeasures. Datafortresses that employ Detection Software only.

The Net: The Cyberpunk 2020 equivalent of the Internet. The Cyberpunk 2020 Net is represented by a 3D full-sensory Virtual Reality. Other names for the Net include the Face, the Cybernet, the Interface, the Web, etc.

Net Access Provider: A company that rents temporary LDL's to Netusers. The Internet Corporation is a large Net Access Provider. NAP's generally cooperate with SysAdmins in discouraging Hacker activity. If an NAP is notified that one of their Netusers is possibly a Hacker, they will discontinue that Netuser's service. The futuristic equivalent of modern day Internet Service Providers.

Netuser: Anyone using the Net legally. The equivalent of the modern Net surfer.

Power: A Fuzion game mechanic meant to be a relative measure of a computer's ability.

Security Level: A Fuzion game mechanic meant to represent the skill used by either a SysAdmin or Computer CPU to deter or capture Hackers. In game terms, Security and Hacking are the same skill used for different purposes.

Server: A computer connected to the Net. The server acts as a middle-man between the person requesting information and the memory storing the information. Your computer sends a request to the server, the server finds it, the server sends the information to your computer.

Speed: A Fuzion game mechanic meant to be a relative measure of a computer's speed.

Stealth Software: Software that attempts to fool Detection Software into authenticating or ignoring an unauthorized Hacker.

Strength: A Fuzion game mechanic meant to be a relative measure of a program application's ability.

SysAdmin: System Administrator. The person in charge of maintaining a Datafortress' security.

System: A collection of computer components that work together. A group of computers attached to a single network would be a system. The Net as a whole might be considered a very large system.

Trace Value: The relative difficulty in tracing a connection's origin.

Virtual Reality Interface: Much like a modern Graphic User Interface (GUI), the VR Interface displays the computer's "Desktop" as a 3D interactive universe around the user. In Cyberpunk 2020, the Net can be accessed in such an interface, displaying Net LDL's as Icons around the user. The user moves freely about in this space, choosing the icon they wish by coming into contact with it with their hands. Their bodies are displayed to them as whatever the user wishes and programs much like a modern cursor, their hands acting as a mouse in space.

VR Construct: A 3D Icon in a VR Interface. A VR construct can be anything, limited only by the imagine of the creator. It's size is determined by how much memory it requires.

VR Sim: A VR Simulation. A tiny virtual universe. In Cyberpunk 2020, VR Sims can be interactive games, advertisements, network conference areas, or fantasy playgrounds. Any situation that requires being someplace you can't actually physically be can be solved with a VR Sim.

by Christian Conkle

References

For more information on other Hacking and Netrunning systems, see:

Cyberpunk 2020 by Mike Pondsmith, R.Talsorian Games.

Bubblegum Crisis RPG by Benjamin Wright, R.Talsorian Games.

NETRUNNING RULES by syberman@syberman.demon.co.uk.

Skyfire Master Force by Gary Townsend, HERO Games.

How Hackers Break In… and How They Are Caught by Carolyn P. Meinel, Scientific American, October 1998.