*** USER ACCOUNTS ***

Instead of directly Hacking a network, crewmembers can gain access to a USER ACCOUNT by obtaining (through theft, intimidation, or otherwise) a user's credentials (e.g., password, ID, badge, PEK, etc.). While having direct access to a User's Account circumvents the need for a Hacking Check, each account is limited in its PERMISSIONS. Here are some examples:

* GUEST ACCOUNTS have very limited permissions, usually only accessing the intranet (if there is one), company directories, or online help.

* EMPLOYEE ACCOUNTS grant permissions over anything in the employee's job description.

  > FOR EXAMPLE: an engineer on a ship may have
  > permission to access the engineering network,
  > and therefore be able to control the ship's
  > thrusters from their terminal.

  Employees typically have access to emails, maps, details about projects, and other company sensitive information and files.

* ADMIN ACCOUNTS oversee several employees, and have access to everything they can access. Admins can be managers, team leaders, IT personel, or officers on a ship.

* SUPER USER ACCOUNTS grants "root" access to everything on the network, and often on several other connected networks.

  > FOR EXAMPLE: A Super User account on a ship
  > would have access to all the ship's networks:
  > utilities, weapons, navigation, employee
  > data... everything.

Super User accounts are a hacker's dream, and often highly guarded or encrypted. However, if your hacker obtains root access to a system, let them go wild, they've earned it.

User accounts can be used in a lot of interesting ways. For example:

* An employee badge might open up all doors on the first few levels of a space station, and then be used to login to a terminal that connects to the station's security network.
* Some networks or devices may not have any user accounts associated with them at all. They can only be hacked manually.
* And of course having access to a specific User Account might provide opportunities to hack Networks unreachable through other means.

Think of User Accounts as a way to engage crewmembers without the Hacking Skill in the actual work of hacking a network.

*** EQUIPMENT ***

-- [Decks]----------
KOMPAN-88 Lomo PX 'Burndeck' 450cr
* Software Slots: 1
* All Nodes at +1 Response
Fedorova-Turner 'Onika' Workstation 1.5kcr
* Software Slots: 2
Bao-Neumann Orion ZX "Superdeck" 3.5kcr
* Software Slots: 5
Sato Bliss 12kcr
* Software Slots: 3
* Treats "Hardened" Nodes as "Secure"
Sinclair 2 .....50kcr
* Software Slots: 3
* Treats Hacking as a Master Skill.
-- [Wristcomms]----------
DVK 'Micro-80X' Printable Timepiece 25cr
* Able to hack doors/airlocks only.
Macrogram 'MX Tattler' 1.5kcr
* Software Slots: 1
König-Seidel 'Series 6' 22kcr
* Software Slots: 2
-- [Gear]----------
Brickboy 300cr
* Portable dongle which fries hardware on triggering event (e.g., door is opened, PDA receives a message, user logs into terminal).
Faraday Bag 75cr
* Small bag that blocks contents from all signals.
Node Detector 750cr
* Detects all Nodes within a 50m radius.
* Scout upgrade (detects node SEC/RES) .....+500cr
Snatcher 150cr
* Copies an entire databank while deleting the original. Takes 1d10 rounds.
Swiper System 200cr
* Printer that duplicates any swiped keycard.
+ Blank Keycards (10-pack) 50cr
+ Credstick upgrade (allows stealing Cr) ....+2kcr
+ Remote upgrade (allows use up to 20m) .....+4kcr
-- [Single-Use Software]----------
CoyBoy 2kcr
* Reduces Response of node by 1d5.
Icebreaker 500cr
* Converts Secure Node into Unsecure Node.
* IB++ upgrade (Hardened -> Unsecure) .....+2kcr
Keylogger 1kcr
* Records all keystrokes, inputs, or button presses on a node. Installation: 1d5 rounds.
Maze 500cr
* Ignores one NetSec Response roll.
Ripper2 .....1kcr
* Brute force password cracker. Takes 3d10 rounds.
Xmap 2kcr
* Retrieves a map of all nodes on a network.

Written by LUKE GEARING
KEVIN WHITLOCK & SEAN McCOY
Thanks to DAVID N. Wilkie
Edited by JARRETT CRADER
mothershipRPG.com

MOTHERSHIP®

SCI-FI HORROR RPG

presents

version 1.1

Hacking in MOTHERSHIP® can be a lucrative, if dangerous, Skill for any crewmember to acquire. It can open doors, control gun turrets, and expose sensitive information. Most *Hacking* Checks are simple: an electronic airlock is locked and the Hacker makes an Intellect (*Hacking*) Check, and if they succeed the door is opened. Easy. However, if a scenario requires a more robust challenge, say hacking into a corporate research station's primary database, the Warden may want to design a **NETWORK**.

-- [D10 Loadouts] ----------

0. 'Onika' workstation (Icebreaker, Ripper2).
1. SMG, node detector, Faraday bag.
2. 'Burndeck' (CoyBoy), vaccsuit, Stimpak.
3. Revolver, crowbar, 'MX Tattler' (Xmap).
4. Electronic tool set, stun baton, Brickboy.
5. Assorted tools, 'Burndeck' (Maze).
6. 'Micro-80X' wristcomm, lockpick set, body cam.
7. Radio jammer, tranq pistol, snatcher.
8. Salvage drone, explosives & detonator.
9. Cat (Synthetic), 'MX Tattler' (Keylogger).

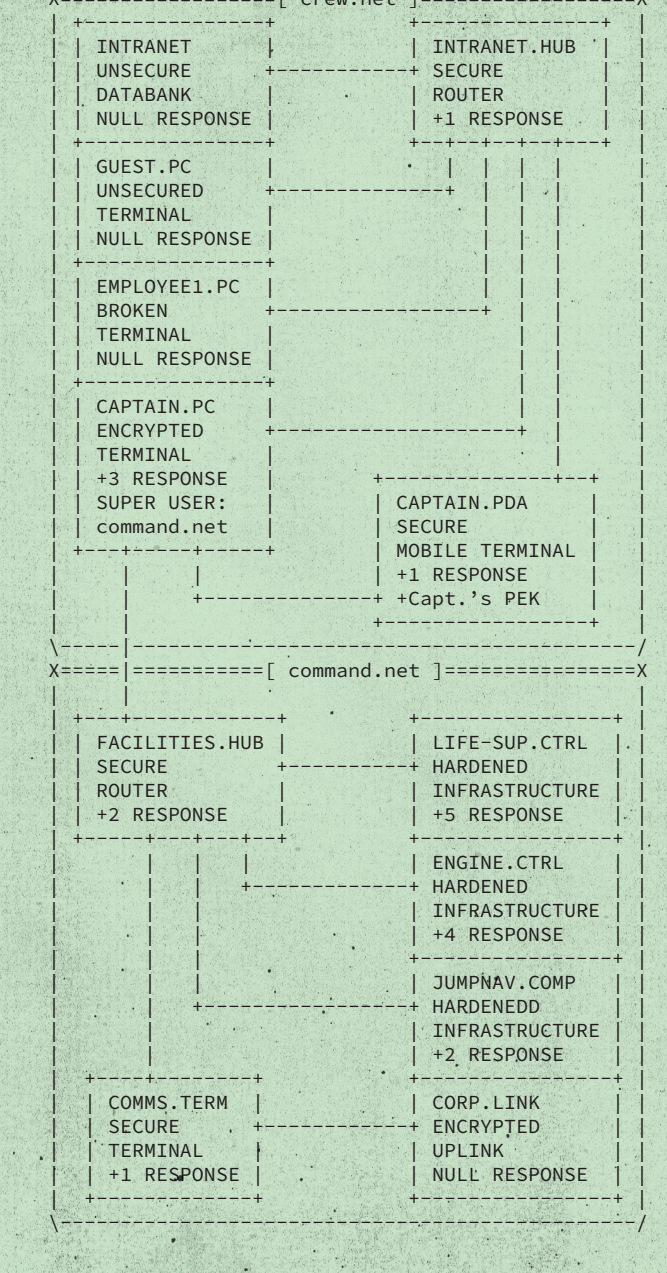
TUESDAY KNIGHT GAMES
MRPG-A1

*** NETWORKS ***

A NETWORK is an interconnected system made up of a series of NODES. Networks can be big and sprawling with dozens of nodes, or they can be small and simple, with only a couple of nodes of note.

-- [Example: J1C-II Research Vessel NOAH-IV]----

This ship has 2 networks (made of 6 nodes each) connected via the captain's encrypted terminal.



*** NODES ***

A node can represent a modems, hub, printer, computer, personal digital assistant, electronically controlled utility, or any other virtual software or connected device.

Each node is defined by its FUNCTION, SECURITY, and RESPONSE.

-- [Function]

FUNCTION is a simple description of what the node does. Several examples include:

* ACCESS POINT: grants entry to the Network.
* DATA STORAGE: contains valuable information (e.g., mission paydata, facility maps, storage manifests, user lists, camera recordings, etc.).
* ROUTER: allows communication to pass through this mode to other nodes connected to it. From a hacking perspective, controlling such a node could allow a hacker to reconfigure network paths to avoid more secure nodes in a network.
* FIREWALL: A high Security and/or high Response Node designed to hinder hacking attemps.
* INFRASTRUCTURE/HARDPOINT CONTROL: grants control of connected location's infrastructure (e.g., airlocks, ventilation, doors, lights, cameras, engines, reactor, life support, weapons, etc.).
* UPLINK/RELAY/BRIDGE: connects one network to one (or more) separate networks.
* TERMINAL: physical interface (e.g., a personal computer) which allows the user to access its own contents and connect to the network.

-- [Security]

A node's SECURITY represents how difficult its defenses are to penetrate. There are four levels:

* UNSECURED NODES are open for anyone to use. They have no password protection or security of any kind.
* SECURED NODES require a Hacking Check to gain access to its contents.
* HARDENED NODES are heavily fortified and require a Hacking [-] Check to defeat.
* ENCRYPTED NODES cannot be hacked with a Hacking Check. Instead they require the PRIVATE ENCYPTION KEY (PEK) of a user who has access to the network. PEKs can be acquired through theft, interrogation, social engineering, or hacking a lower security node (like the target's personal computer) which contains the PEK.

These four levels allow you to quickly establish how hard the hack will be and communicate that to the hacker so they know what they're up against.

--- [Response]

A network's RESPONSE measures how severe the reaction is from any network admins, operators, automated security features, overseer AIs, etc. safeguarding the network. RESPONSE is rated from Null (no roll required) to +5 (a rapid and severe response).

Whenever a hacker fails their Hacking Check, roll on the RESPONSE TABLE and add the Network's Response.

+--------------=[RESPONSE TABLE]=--------------+

D10	RESPONSE
00	Warning message. Network's RESPONSE +1
01	Device is remotely powered off.
02	USER ACCOUNT locked out for 1d10 hours.
03	Security member dispatched to investigate. Arrives in 1d10 rounds.
04	Network creates "dummy" directories for the Hacker to search while a security team is sent to investigate.
05	The network and all linked networks are locked down for 1d10 hours.
06	This network and all linked networks increase security level by 1.
07	All linked networks increase RESPONSE +1
08	Facility blackout. All non-essential electronics powered down.
09+	TACTICAL RESPONSE TEAM deployed on Seek & Destroy mission. Arrives, heavily armed, in 1d5 rounds.

Other examples of Responses include:

* DENIAL OF SERVICE: NetSec blocks connections from the hacker's connected hardware by flooding the connection with garbage making future hacking attempts slower.
* BACK HACK: NetSec attempts to control/destroy the terminal/deck/etc. being used in the attack.
* MALWARE ATTACK: NetSec uses a virus to disable the hacker's hardware for some time.
* POWER OVERLOAD: NetSec pushes excessive voltage to the hacker's hardware.
* IDENTITY TRACE: NetSec attempts to obtain identifying information about the hacker.
* NETWORK TRACE: NetSec attempts to locate the physical location hacker.