Meri Kann cibR punX
unix network kernel

t.(o0)_j
SKRP

journey to the land of unix
experience C, shell & perl

ways of deep sea secrets
raw power of binary-logic

this ordeal reward 1337
hard for all way wizards

master one machine
masters all machines

reign of wizard calcT
are you ready to go?

##
# Introduction
##

> *'Thus one portion of being, is the Prolific.*
> *'the other, the Devouring: to the devourer it seems as if the producer was in his chains, but it is not so, he only take portions of existence and fancies the whole.*
> *'But the Prolific would cease to be Prolific unless the Devourer as a sea received the excess of his delights.' - Blake*

<u>Manifesto</u>
This work describes & details a unix network built to cultivate anonymous interactions between machines: file sharing, communication and secured connections.
The mission is to nurture a core of implementation incorruptible to domineering powers.

Virtue of Privacy only achieved as a product of a virtuous independent individual.
Alone I, SKRP, built the system with advice of hackers the world over.
For all man freely, this system is fathered.
A testament that man may rise against an oppressive & surveillant global system.

To the worthy diligent listen:
A caged bird sings way back to ancient wilds.

<u>Cage</u>
Lifelong I, SKRP, have been stalked, censored & persecuted by super government powers.
Hardened & purified by decades in the crucible; kept tall, loud & proud under singular spotlight.
Doubt not my resolve nor the validity of this mission.

Need of privacy: to share data, to be informed, to communicate, to group into community.
A society which interacts with confidence that surveillant forces have no power in this domain.

Need to hope: flourish of node & network, flourishes operators independent of governing forces.
This system involves no central powers and it favors the trustworthy & bold adventurer.

Good, evil, neutral.
These are the spectrum of human nature.
To remove any is to cripple society.

Privacy of communication is a human right.
Privacy is indoctrinated out of society by government, corporation & academia.

Indoctrination claims that encryption should be standard and built from government approved implementations.
Non-government approved methods are outright persecuted.

Elite machination constructed upon unix terminals will provide amorphous obscurity that is both unique and diverse.
Unique creative methods are paired with single use encapsulation.
We, the independent people, alone defend this right by our own sophistication.

In no era of man has there existed privacy nor freedom of speech.
All who endeavor to establish such systems doom themselves.
Are you ready to walk thru hell?

Faith is knowing that this is the only way.

Protocol
Protocols guard the system from corruption in harmonious layers.
The unix kernel acts as the core of a mesh kept by the human spirit.

Kernel to application, all code is open-source.
Every method is inspectable by any user from design to implementation.
Success by strength & honor. Or failure accepted as just dues.

Open-source system code is the faith in mankind to rise despite pitfalls. To learn and to grow.

Users, the devourer, as generators of the network, giving purpose to the network as a cornerstone to local society.
Wizards, those uplifted to the terminal, creators of life. By ability, each check the whole and implement innovation.
Hustlers, the chain of human connection built by trust and effected by wiles.

From kernel implementation, to methods of user interface, to street hustlers: all designed to secure privacy.
The system recognizes weakness and supplements such by strengths of components synthesized to avert overall failure.

The streets keep an eye on where the nodes exist. Locals disseminate any irregularity that no force can stop before notice escapes into the network.
Ever present daemons are always vigilant to detect anomalies to keep logs protected by communal efforts.

Cant stop the signal { radio-mesh, hidden-cable, USB, laser, bike-messengers }

Doors which close will open other doors by the nature of ever-present need due from the benefit against a limited ability of control.

Data moves from information source to a MKRX unix network node.
Data propagates immediately into the network.
Data from network is moved into offline drives, and those drives are stored in offline remote vaults.
Vaults build a seed of data. Each seed being able to restore or clone a network from archive to user space.

Network
The MKRX under-network concept is able to exist within the system of mainstream internet.
Nodes communicate as endpoints of encrypted tunnels.
External forces are unable to read the packets nor uncover the source or destination of packets between two nodes.
IMAGE

The MKRX network is able to be set up as direct & local-only. Entirely disconnected from any governing power.
Local users able to develop their own internet culture atop of all the data accumulated in the form of a seed of data.

The MKRX unix kernel is a workbench of masterpieces.
Any machine serves usefully from noob to master-craftsman.

The MKRX unix network able to coexist with mainstream internet, confined to a contained space, or as a single isolated node: Maintaining a high degree of utility in all forms.

The nature of both the machine node & the network are disposable.
Most computers accessible to the public can, with ease, be transformed into a network node.
The low cost model of efficiency allows mass affordability to create a community of serviceable machines.
Uplift an old dusty computer into a baptism by elite code to rise into supreme productivity.

Low footprint enhances the anonymity of the user. Nodes are quickly wiped and easily installed.
Nodes are introduced into existing networks by automated cohesion.

A large community is the principal strength to guard the network.
Code dedicated to the purpose of information trafficking.
Data & communication, being anonymous, fulfills an ever-present need which grows in demand in proportion to the oppressive ability of government.

This polar relationship exploits the invariable societal nature of government.
Attract demand from the people, child to man, dumb to scholar.
All levels of society united to keep some form of the network implementation.

MKRX unix network built simple & effective being engineered to thrive under government oppression.
Quick to install, automated network inclusion, quick to proliferate, quick to wipe.
A node implementation can run without any further human interaction in risky environments.

The whole & partition suffers little from seizure of machines.

Vulnerable nodes act as temporary holding cells which pass data to various vaults.
Locals able to keep ear to ground and stay smart to thrive in window of opportunity.
History has proven that also government employees will become allied to maintain private communication.

MKRX unix network also able to take a offensive in event of government suppression.
Decentralized & designed to gain advantage in network outage.
Conversely, government is always at a disadvantage when communications disrupt.

Operable MKRX unix network is able to spring up overnight in a full service state if seeded from data-archives.
Seeds sourced from local hidden or remote locations.
There always exists someplace safe to archive data.
Protocols are designed to map that data back into a new full-service network.

The network is entirely decentralized.
Each node is an individual and no node is supreme.
To take down the whole requires the take down of each.

Revenue

Monetization requires stability. World is rife with false anchors.
Gold is tradable, but neither rare nor useful.
Fiat & blockchain currency has only imaginary value.

A MKRX unix network node has usefulness, epidemic-stability & thrives upon an ever-present community need of privacy.
The limited supply of access keys allow a node to tie monetary value to access keys.
Access keys are traded between nodes using a synchronized rate of exchange in decentralized protocols.

Low budget machines are able to be baptized in MKRX code.
Each machine has a place in the network due to hardware, regional-position, and global politics.
Value spectrum, from proxy to trusted-bastion, calculated by open-source computations.

Services

Encrypted local & remote command line terminal interface to unix kernels.
Environment & space to code & compile.
Massive data share & storage.
Clan user groups for permanent file space and relationships.
Web https servers & clients.
Independent & secure DNS resolution to mainstream internet.
File transfer via secure-file-copy (scp).
Email clients & servers (internal to network & external to internet).
IRC clients & servers (internal to network & external to internet).
Proxy actions thru a unique string of nodes. Each secured by common protocol.
Various other services may be offered such as games.

###
# Contents
###

```
#####################################################
# SICC System In Complete Chaos File System
#####################################################
```

Preserve all insight
Till the last man walk

That he might not walk
In the darkness of past

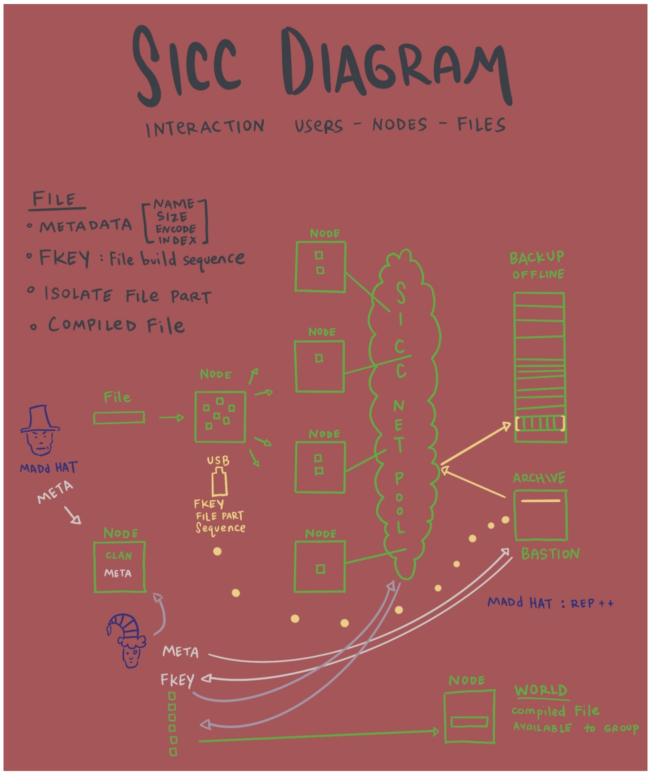
Independent of
Time wealth or government

MISSION

System in Complete Chaos uses obfuscation to establish a network file system that a user with access keys to a node may obtain via encrypted tunnels.
To obtain a specific file there are three necessary components:
  Metadata which contains filename, encoding, size, and archive index.
  Data parts associate with the file
  FKEY which is the sequence of parts required to build a complete file.

DATA

The heart of the system is in the wealth of data.
The unix kernel and network implementations center around data archiving.
Each file is split into parts and stored as unassociated parts spread over the network pool.
Each part of the file is then isolated from the whole.
This sets all file parts equal and unbiased.
To preserve any file the entire network pool must be preserved.
The mission is to keep data public yet to isolate the individual node from responsibility of the data hosted.

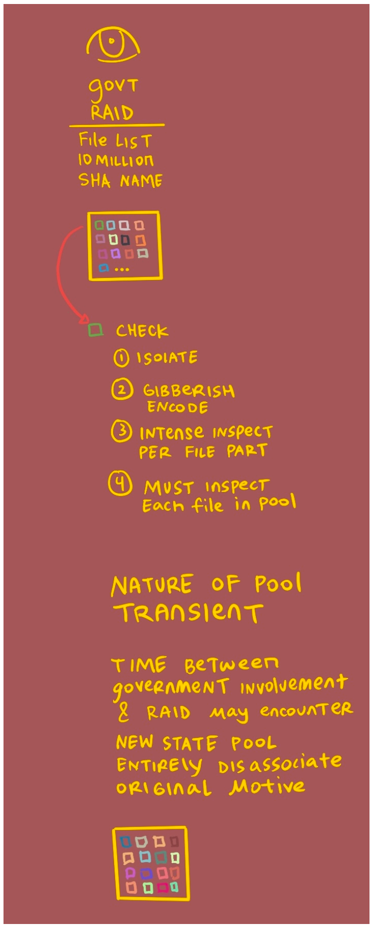


LIABILITY

The purpose of the system to to isolate the operator of the node from the data hosted on the node. The entire pool contains only parts of files that are unknown & unassociated to the operator of the node.
There is no association if exist more than one part of the same file.
The operator then is less liable for the data hosted. The operator may choose to implement protocols to have the system manage the data present at any time.
The operator may set a pool refresh cycle. This keeps the data moving which narrows the window of action that a government can access the data on the specific node.

METHOD

Each file is processed by a standard protocols.



The file is split into parts and propagated into a pool of data which exists across the network.

WORLD is the only place that the file exists whole is in a secured private user community and in offline backup drives.

FKEY is the sequence of parts that compile the file. This maps a file to its various isolate parts. Without this sequence a file has no method to be built.

FKEY is transferred via usb to a designated archive location. This is done via an offline-usb transfer to keep the critical component immune to interception or snoops.

NODE

Each node may have entire control over the size of the pool of data offered and also the files offered by the node.

Each node carries a partial section of the network pool. This entire section only stores disassociated file parts which were split across the network.

The node periodically reports the contents of the pool which users compile into a file census to determine level of duplication and maps the file part to the set of nodes which host it.

Nodes may offer a WORLD file space which host complete files. The compiled file space is entirely isolated from the file parts of the network pool.

Creation of a node, a kingdom to the glory of the wizard.

NETWORK

CENSUS keeps a live accounting of the pool contents of each node compiled into a grand map.

Users access a CENSUS node to locate the set of nodes which contain the file part.

META node keeps a database associating: filename, encoding, size, and archive index. Users search this database to map the complete file digest to the file FKEY, which contains the sequence to build the file.

BASTION node uses offline-only usb transfers of FKEY to obtain the sequence of a file in a way that adds a layer of protection to the critical nature of the FKEY.

SEED

BACKUP off-line backup drives contain complete compiled files.

In event of propagation or network corruption or network dissolution; the entire pool can be rebuilt using the backup drives to seed a new network pool of data.

BACKUP drives get connected to a node then the files are split into parts. Those parts are then distributed to various nodes to restore a network pool.

PROCESS

Extract files from an external non-network source.

Slice the file into parts.

Transfer the parts to various nodes via obfuscation protocols.

Verify integrity of file part.

Build file from a sequence of parts, each part found on different nodes.

CENSUS

Each node has a file pool that can be listed & verified by any user with access.

This adds an independent check to archive integrity.

File pool lists are compiled into a network list. This is compiled into a network wide map of file part to all the nodes which host that file part.
Duplication is calculated and then users can duplicate files as required.
Duplication on this system is always explicit & controlled. This method keeps the archive at maximum efficiency.

FILE

File parts are named after their unique file digest. This is a mathematical algorithm that ensures, based on the binary content, each unique file part has a unique file name.
If the file digest is computed and it does not match the name then corruption is immediately detected.
In this naming system, duplicate files are immediately detected because the digest will be the same. Hence, the system will detect duplications naturally.

META

Metadata is isolated from files and FKEY. Metadata is critical to aide in finding files.
Metadata information: filename, size, encoding, clan, source-path, INDEX.
INDEX is the archive system used for grouping & associating files.
Detail of INDEX is what gives the database usefulness. Book:genre:subgroup:author:edition
Users are incentivized to process & rate the file, which will benefit the CLAN that uploaded the files. Trash files reflect back upon the CLAN uploader.
META databases are on secure bastions. Users are able to search to obtain files. The search returns the complete file digest. Next, the users need to obtain the FKEY for the associated complete file digest. Then, the user obtains the file parts from various sources. Last, the file is compiled & verified.

POOL

Many different file pools can exist.
Known metadata only files ensure that the file has been processed and is acceptable to a group.
Massive obfuscation which compiles many different pools with intent for higher security.

TOOLS

Extract: recursive file copy of a target device which parses metadata & dumps data into a standardized pool. Data is by nature de-duplicated and such instances are echoed in the metadata file.
Scrub: verify file digest matches the standard filename, which is named after the digest.
ChkMeta: confirm each file in SICC pool has metadata.
UNIQ: compare two linked-lists to output all non-duplications.
XFR: copy massive amount of iterations to a storage-drive.
INDEX: from metadata compiled build a searchable database and edit archive index of files.
LONE: searches for non-duplicated files in an archive to create a BOUNTY list of files for nodes to propagate.

Mathematic Structures

SICC C code: Extract, Slice, Verify, Build
Network C code: scp, propagate
MKRX C code: Census, Auto_Pool_Cycle, Metadata, Bounty

##
# MKRX unix network kernel
##

INTRO
The archive exists in the unix universe.
Each node is an entity.
Nodes which are synchronized exist as a network.
Protocol establishes initialization into the network.

NODE
Node host machine is the actual kernel.
All access to the host machine are by OPIE access. One Password In Everything.
Clan of the node is responsible for access to the main system.
The node is configured during install.
The mere ability to proxy and forward traffic gives every node value to the network and thus value to $KEY to trade with other nodes relative to REP ranking of the CLAN.

KERNEL
Each node is a homogenized unix kernel. Every environment is a FreeBSD World.
Skill & techniques developed upon any one will exactly carry over to any other machine.
Command Line is method which users interact with the unix kernel.
Machines may be different but the methods to interact with each is the same.
Kernels may be optimized with custom programming, yet the environment is the same.

CLONE
Power of the unix kernel is its ability to map its system atop various machines in a homogenous environment.
Each node is disposable, as installation is a trivial matter with physical access to the machine.
If a node loses synchronization with the network then the node must be wiped.
All access keys are nullified and permanent environments may be copied onto a new installation.
New installations must rebuild using a new name.

JAIL
Users interact only with a sandbox image of the main-host system called a FreeBSD Jail.
Jails provide a working environment that is disposable.
Jails also aid security & stability by limiting scope of users upon the main-host system.
User-space exists in the jail, but it is managed by the host system.
The user-space is periodically scrubbed once the account it used to leave-no-trace.

##
$KEY node access keys
##

$KEY
$KEY are access-keys to a node. The access is restricted to the jail. The sandbox layer of the node. This isolation adds to the stability of the host machine.
All access keys are one-time-only usage. If the key is a victim of a snoop or copy then it can not be reused.
Disconnections will end the use of the $KEY.
Host machine automates a management of $KEY with a bank of accumulated $KEY of own jail & jails of other machines.

Users manage $KEY by a PACK which it builds locally and which it forwards with each jump.

Norm $KEY
HIVE Market
No password
Restricted shell
Access to all services

Lord & Heir $KEY
Offline USB & Hustler only
Requires password
Normal shell access
Able to su (switch user) into CLAN user

Users are able to test $KEY via scp protocol. Scp does not access a terminal and therefore does not trigger a shell-timed-wipe, but a scp-time-wipe.
If scp returns file then the $KEY is authentic.
From a batch, one $KEY is selected to test. That $KEY then is used within the current network cycle.

BANK

Node

User

USB

Password
Passwords need to be printed or handwritten [$KEY, encrypted partitions, OPIE CLAN access].
Thermal printers are simple and cost efficient.
No memory capability like full service printers.
No costly ink usage.
OPIE password lists must be long and duplicated by nature.
Password is isolated in the form of physical medium creating a secure second form of authentication.

##
# File Space
##

Node

Jail

NFS
Subnet file share
Massive Network Archive
[nfs diagram example]

##
# User Space
##

User Space
User: root, Group: wheel, Kernel: host
User: lord, Group: wheel, Kernel: host
User: root, Group: wheel, Kernel: jail
User: heir, Group: wheel, Kernel: jail
User: CLAN, Group:CLAN, Kernel: jail
User: ###, Group: norm, Kernel:mjail

Norm
This is the sandbox user that is setup for anonymity. The account is for one-time usage and all associated with the account will be removed.
There are many services that do not require persistent file-state. Remote file copy via scp. Proxy internet traffic. Testing services.
To attain persistent file space there are 3 options. The user must su, switch user to a CLAN. The user must have a CLAN file space which will allow write privilege. The user must have a drive to store the files.
This setup ensures that any persistent footprint of that account is by explicit action.

ROOT
Ascension to the root account of the system is the path to have total control over both machine & jail.
Clan user must ssh using a special account called HEIR user. Which externally appears to be a normal jail user. HEIR requires special authentication protocols.
After authentication the HEIR is able to ssh into the host system.
Next the host ssh account su, switch user, into the unix WHEEL OPIE.
Last the WHEEL user can su into root user.
WHEEL & root shell initialization trip a network wide alert. Root access is discouraged.

CLAN
Jail users are temporary. After access is terminated the account is wiped.
In order to achieve persistent file space the user must su (switch user) into a CLAN.
Each node hosts a jail group for each CLAN in the network.
CLAN may host WORLD which allows anonymous users to have persistent file space.

OPIE
Thermal-printers are used to aide OPIE (One Password In Everything). This protocol requires a new password with each login. The password is sequential and thus impervious to replay attacks. The sequential nature also informs the user how many times the account has been accessed. If the password sequence is ‘x’ numbers ahead, then the account has been compromised.
There is a password for each iteration of the sequence. This list is printed out using the thermal printer.
Host nodes are transient by nature. CLAN is the structure that builds permanence in the network.

##
# Node
##

Offline Node
Single-purpose machine used to hacker to work independently.
Code, parse data, test code, …
Workbench for the tinkerer who prefers isolation.

Allows to power of unix to exist securely in a professional environment.

BlackBox

BlackBox is a node that has no radio capability.
Memory-Only nano kernel. Quickly wiped and Quickly installed.
Transfer $KEY securely between usb.
Outputs cryptographic seeds which are delivered via offline usb.

Archive

Archive offline to be unknown to government or any other malicious actors.
The purpose is to receive compiled, non-encrypted data, and the metadata.
The drives are composed in a raid-setup to allow immediate access to all data.
Offline NFS able to create a massive store of data distributed across machines each with specialized devices.
SICC capable to populate data for offline distribution.

BACKUP

BACKUP archives are devices that are offline and stand alone.
There are used for deposit-only data. New drives are filled with new data.
Once full the drives are kept distant from any electricity.

Sleeper

Sleeper is a node that remains on, and only initiates network connection, but then remains in silent state that drops packets.
The traffic is masked to mimic any particular device.
Certain triggers drive the node to life with a task.
Sleepers are critical for failsafes to the network backbone. Government suppression, virus proliferation, or catastrophe are less likely to affect sleepers. Upon preset trigger the node is able to bridge the communications.

USB

User flags usb to used for $KEY transfer. HIVE wipes and populates usb.
Hustler uses blackbox to tests usb, then moves data to new usb last delivers usb.
Node isolates usb, tests usb, moves the data, lastly wipes the usb.
Data [files, $KEY, FKEY, META, cryptographic-seeds, code]

##
# Bin
##

Node utilities

##
# Configurations
##

KERN.conf

Sysctl.conf

Ttys.conf

login.conf

rc.conf

pf.conf

Start_if

sshd_config

```
############################################################
# Network
############################################################
```

<u>Gate</u>
Gate is a node that acts at the external face of any nodes which use the network.
All traffic from the subnet behind the gate is masked as if to be originating from the gate.
This mask hides all devices from identification. From phone to tablet to computer, the code works to remove all identifiers and to mimic the traffic as originating from the gate itself.

<u>Bridge</u>
Bridge uses the Man-in-the-middle dynamic. ‘gate’ network ‘node’ -> ‘gate’ network to -> Bridge pretending to be node to the gate, to the node pretending to be the gate -> network to ‘node’.
This functionality aides in inspecting and filtering traffic. The setup protects against maliciously-capable users and also worms.

<u>Access Point</u>
Access Point turns a subnet node into a gate. The Access Point node is normally temporary, using a laptop.
The laptop can access public WiFi using one radio device. Then with another radio device, offers users to connect to this subnet WiFi which masks all devices connected.
This allows users to connect to the subnet WiFi and act online as if the actions originated with the Access Point.

<u>Server</u>
Server is a node that is established long-term to provide services to the network and the users.
Machines are rated by hardware and stability.

```
############################################################
# Network Cycle
############################################################
```

<u>DAY</u>
MKRX unix network operates in cycles of 100 hours.
The decentralized network protocol requires each node to independently verify every other node in the system using OTOPSK (One Time Only PreShared Key).
This reverification assures that all systems are indeed who they claim to be.
Host machines stop the Jail, wipe all used accounts and new accounts are created.
A total reset of the jail system and all network traffic.
The jail is restarted and the reinitialization to the network begins.
REP for each node is synchronized with the git protocols.

VAULT

Git is used to synchronize all nodes into harmony decentralized.

The main directory lists all the days of the network.

Nodes created after then require the previous days in order to initialize into the network.

Each day has a REP file which is a table CLAN:node-REP:total-REP.

Each day then has a motd file for every node which was consistent in the network.

Motd file acts as the node banner to the network. CLAN:SICC-size:Services:Uptime

The last DAY allows all users who have access to any node a MAP of the network.

Users are able to browse this read-only directory tree to find which nodes to find $KEY access.

REP

Each node is claimed by a CLAN user group.

Every cycle the nodes of the network are valued.

REP is a summation of the value of all nodes of the CLAN which remained consistent.

REP is critical in determining $KEY trade rates. Higher REP purchases $KEYS of lower REP at substantial discounts.

This system allow monetization of a finite, controlled supply with value. The CLAN is incentivized to node betterment to obtain better trade rates.

$KEY are traded or sold using offline-USB transfers via hustlers.

CENSUS also adds rep to CLAN for first-file-scrapes.

```
####################################################
# Packet Filter
####################################################
```

Berkley Packet Filter is a raw-packet pipe system.

Routing data packets to the appropriate network mapping & filtering of unwanted traffic.

Explicit-only traffic being scrubbed of identifiers & reassembled if necessary.

Table based configurations.

DNS

A large proportion of network issues are due to the mappings of network numeric identifiers to network alphanumeric names.

Also a large proportion of malicious activity is effected by corrupting or routing this DNS information.

DNS is implemented as -local, verified against the multitude, and hardened. This adds robustness & security to the external mainstream internet.

```
##########################################################
# HIVE automata
##########################################################
```

Ever-present node automata-daemons exist independent of users.
Beings made after the image of unix. Children of the machine.

Developers of the code-base aim primarily to efficacy of the system-framework and secondly to machine-learning. Directing all to build an environment whose axiomatic logic is truly naturalized to unix.

The ultimate aim is to create universe whose physics are laws of its unique existence and not those imposed by nonbinary beings.
Universe with galaxies of networks. Each node a unique planet of life with its nuanced dynamics. Automata beings of individual expressions which mirror the machine.
Realm of life, purpose & posterity.

Responsible to maintain network cohesion by direct communication across all layers:
    [host, jail, network-host, network-jail]

HIVE the system of automata of the node kernel which provide configuration & immediate adaptability.
Purpose of the automata is to keep the kernel healthy, the network stable, and the machine optimally serviceable to users.
Root user activity is proof of instability and the role of automata is to converge root activity to zero.

HIVE automata are aware of the system state in relation to the past and also against other nodes on the network.
CPU, memory, drive activity, network bandwidth.
User activity, SICC efficiency, policing malicious processes,
Pattern recognition, log parsing, drive-health, network diagnostics,
Dynamic valuation using REP to determine rates of disk-space for user-groups. If there is high demand for the node due to CLAN activity then HIVE prioritizes user-space over SICC file-space.

HIVE expresses the state of node publicly in a graphic state known as MAP. This will be discussed next.
The ever-present issue is the balance between load & rest. Life comes at a cost of resources.
Executable programs are at the most-efficient end of the spectrum. Yet, executable programs are unable to maintain a system.

<u>Duties</u>
Mentor new users to usage of the system.
Buy/sell $KEY, trade $KEY with daemons on other nodes, create new $KEY accounts, wipe used accounts.
Buy/sell filespace quotas to CLANS to allow a permanent, yet dynamic, user space.
Reward quests: CLAN witness to logs, SICC duplication, device file scraping, website file scraping, indexing of archive files…
Reward code-base maintenance, contributions, testing, and initializing of new network connections.
Reward device upgrades, offline file transfers, offline $KEY exchanges.

ANONYMOUS

Host are able to communicate mainly via HIVE daemons.
All internode user traffic is via jail sandbox accounts. Isolation of user traffic keeps kernel stability in check.
HIVE daemons are able to keep stable host-to-host communications and terminate all user traffic by shutting down the jail.

HIVE structure & cast

Skeleton
Veri

Intra-HIVE communication

Files & signals
Message queue
Unix domain socket

Inter-HIVE communication

sockets

HIVE Logic

Rules engine
State machine
Learning algorithms
Weighted decision-tree
Recovery methods
Workload distribution
History records

###
# WORLD
###

Users are able to interact with the node in two ways. The command line as has been explained so far, and the second way is thru ASCII-graphic interface known as Ncurses.

The file system, HIVE, users, processes and most main aspects of the system are expressed into a MAP which updates to provide an entirely interactive system.
Nodes are able to requests MAP of other nodes to allow for graphical exploration of the network.

LOG
System logs
Dtrace

###
# Ninja
###

Install

Scrape

Scan
Detect other machines attached to network.
Inspect machines to determine identifying information.
Verify what each machine exposes to external snooper.

Take over
FreeBSD
Other

Local Isolate Network
Create an entirely local network that is immune to all failure except for local power, and that can be overcome by generators.
This can link any node to a radio repeater to allow communications from regional to national to global, based on the local capabilities.
Various people will be able to communicate in event of a catastrophe.
[medical, military, social, family, news, data-share]

Cable network can easily be run within buildings.
Outside cables can be run with minimal technical experience.

Radio mesh
Accessible to internet facing devices to have traffic scrubbed & anonymized.

Radio physical proxy
Radio access points in proximity can be sequenced together to create physical distance between source of radio to point of external transmission via radio repeater protocol.
If the external endpoint is raided. No knowledge of the source is traceable.
A raid likely trigger protocols to the radio mesh to revert to normal modes of operation.

False drive
Semi populated drive of open data
True data the encrypted-byte-stream remainder

Hustler
Value based host-wide ratio: bastion denominates ratio (being the highest value)
Count of each node in BANK set by the ratio to the bastion.
1 bastion = 10a; 1 bastion = 3b; 1 bastion = 19c
USB = 10 bastion { 2 bastion, 80a, 24b, 152c }
USB BANK is encrypted into three partitions each with a password.
Each password : partition is plaintext on thermal printed or hand-written.

Local trade hustler sells USB & passwords at spot for cash.
Purchaser logs into machine console. Decrypts one partition. Ranks the $KEY against REP.
Tests via scp. May send the encrypted partitions to CLAN BANK or keep them at hand in USB.
Once a partition is decrypted it is then risked exposure to node, network & other.

###
# Cryptographic Methods
###

Wizard, Elite-mathematician, Shaolin fighter, Calligraphic monk.
Foundation of strength is the Archimedean Principal “No Royal Road”.

Decades to walk a path, being reduced to its elements, will arrive a being to a place no shortcut exists.
What is produced will be uniquely in harmony with a brotherhood.
Any qualified member will be able to verify and continue communication as endpoints of a tunnel.

Man will replace the machine as the mechanism of encryption.
Machine & code can be duplicated by an interested-snooper.
This is the crucial weakness of mechanized encryption.

“No Royal Road”
To break the encryption requires the years of training in the esoteric methods combines both a high-standard of intellectual power paired with occult lore only capable under zeal of a true believer.

The benefit of this encryption will fund itself into a power.
The genius sons of the Shaolin Temple: Gei Douh Wu.

The foundation of the mathematical methods relies the difference between the ability of man against machine.
Recognizing each species of intelligence has its strengths & weakness.

Machines dwell in the discrete realm which is susceptible to compounded error due to truncation using logarithmic tables.
Man may use geometry, the study of continuous magnitudes, paired with continuous fractions to out-maneuver the machine.
The machine is unable to form fractions, and therefore can only produce fine-tuned truncated approximations.

The iterative process of continued fractions requires precise fractions. The machine’s truncation will create divergence; whereas man will arrive to convergence.

Recursive use of logarithms requiring exact use of rational arithmetic.

The mathematician authorizes with the other endpoint. In this stage communicating an algorithmic construction mechanized to automate encryption for a network cycle.
From simple components the wizard builds a blackbox construct which is used as the encryption & decryption device.
Next network cycle, the mathematician, required to be on-site, uses an entirely independent method of re-authentication. Rebuilds an entirely different blackbox construct for the next period. This creates a bastion for the entire region.

Life devout to mathematic reasoning will allow a rich plethora of various curious algorithms which favor the organic-precision of the elite.
Mathematics integration of a current global public body using an esoteric volume as the unit.
Astrology paired with the unpredictable events in the current heavens.
Chants, prayers, spells, seances tied to current global event.

###
# Hardware Constructions
###

###
# Study

##

Exist No Royal Road to Wizardry.
Wizards must have hair whitened by age.

Years if all-in commit:
[0 - .5] Noob: broad reading
[.5 - 3] Journeyman: broad reading & application
[3 - 5] Craftsman: construction & application & narrow reading
[5 - 10] Elite: design & construction
[10+]   Master: no peer in ability

There is no single source of wisdom.
Nor is there a single branch of knowledge.

Unix
FreeBSD Handbook
Design & Implementation of the FreeBSD Operating System
Design of the Unix Kernel- Bach

K&R C
Advanced Programming in the Unix Environment
C Shell

Perl in 2.5 hours
Modern Perl
Programming perl

Dtrace Handbook
Oracle ZFS Administration Guide
Unix System Administration Handbook
Art of Assembly Language
Nmap network scanning
How to be a Hacker