WIP: This article is a work in progress and is not yet approved for usage in the RP.

Applications for the Lazarus LA+ LAPLACE Operating System

Applications are software usually with a highly specific purpose in mind. They focus largely on a model of manual interaction, per-step feedback and are the local or client-side of software.

System Interface Software

Software used in the control of LAPLACE to feed suggestions and commands into the system.

AEUS

Converts textural description and simple graphics into a tangible experience via neural suggestion: A form of willing' hypnosis which replaces conventional experiences of reality. The backbone of LAPLACE's augmented and virtual reality systems.

MONOS

Mixed self-Optimizing Neural Operational System: Essentially the backbone of LAPLACE's neural interface.

AXNIS

A simple terminal prompt. Can be paired with MONOS for low-level high-authentication core system & kernel commands.

Exnix

A simple rapid-fire input system which plugs into MONOS. Essentially it works by creating simple silent neural sentences using nouns (target objects), verbs (an action performed on that object), adjectives (a measurable quantity). Simple logical steps can also be introduced in the same sentencing system if 'scripted' can be visualised as a flow-diagram. It is essentially a simple form of scripting.

Example commands:

- “Prevent engine temperature from to raising above 400 degrees”
- “Notify me when target enters vicinity.”
- “Distance to target?”
- “Reboot the server in 20 minutes”
- “Match stop-velocity to target velocity”:
  - Throttle at zero means matched speed. Above means to move faster, below. Ideal when trying to tail or follow something.
- “Match relative position to target”:
  - Vernier control is set to automatic: 'Still' condition is following target. All actions are relative to its position.

Axnis

A terminal prompt system allowing for deep low-level highly authenticated instructions to the kernel itself and software, overriding many common restrictions. A favourite of sysadmins.

Grapher

A pattern-recognition system designed to look at massive amounts of raw data and indicate discernible patterns and trends. Works best when used with BNLSL.

Adjutant

A specially formed and designed ROM Construct with components from many people, acting as a base intelligence for the management of LA+'s actions - parsing and automating a wide variety of actions. It is highly simplified compared to network entities and unlike them, doesn't require access to the Lazarus Processing Network in order to function.

- **Current version:** 0.8β, nightly

Processing Software

Software which is used as a compatibility layer between instructions and actions.

Otheros

A dynamically formed compatibility layer to run software from other operating systems as a native first-class application. The interface output of applications running in Otheros are read and reconstructed, depicted using LA+'s own native interface elements. In addition, MONOS instruction and semantic library sharing is also implemented - allowing these existing applications to work in ways they traditionally cannot.

Compatible software includes software designed for…

- Kessaku OS
- Nekovalkyjra OS
- KAMI
- MIKO
- Kesslinger Intelligent OS
- Lorath Neural OS
- Freespace OS
- Skylight OS

ARIA

Allows for sandboxed realtime execution of the ARIA platform including the ROM Construct platform. ARIA instances can be modified and loaded from saved states, fast-forward or rewound. Often if a user is unfamiliar with software, a construct will familiarise itself with the software within a few hours and be able to act as the go-between user and application to a limited degree.

- **Current version:** 0.6.8 β, nightly

General Purpose

User-written software specially written for the platform.

XTAL

XTAL (Multipurpose Telecommunications Artificial intelligence Layer) is an adaptation of the networking technology from the M1 Hunter - now rendered an AI expert-system. It excels in tactical and situational information distribution - ensuring that two computers in entirely different locations have an idea of what the other and its target platform is going through with contextual intelligence - ideal for large vehicles and machinery.

Bodsim

An application used to monitor the effects of various events on different physical anatomies. From crash-tests to medicines. Ever wondered what happens to a person inside a black-hole? Feed the conditions to

bodsim and let the simulation roll.

YumeChat

A chat procotol system which translates neural information into AEUS meta-data, essentially allowing for a sort of bounded collective experience, similar to people dreaming together. The name is derived from the Yamataian word 'yume' meaning 'to dream'

Design Software

Software which aids a user with the design process. Often demands a lot of manual input and requires user expertise on a topic in order to be leveraged properly. Unfortunately it can be incredibly demanding and has a low priority on the network due to the length and size of tasks requested. As such, it is recommended a user build their own private hub or workstation for use with Oedo. A number of closed source applications used only by the Consortium have not been included in the public release and thus have not been listed below.

Oedo

A comprehensive CAD design and editing suite with physical simulation capabilities - produced by Lazarus. Specially designed for use with a Lazarus molecular applicator - able to 3D print incredibly small and precise objects or large components in almost any material imaginable.

- Macro-scale design of static and dynamic objects
- Circuit, pathway and systems design
- Software Design
- Nanochemical design
- Chemical simulation
- Field system emulation
- Quantum system simulation

Monkey

An application used to perform advanced physical simulations and stress-tests to find potential weaknesses and issues in designed hardware. Named so because it essentially submits the hardware to a simulated idiot out to break your hardware through any means necessary - known as “the monkey” - literally idiot-proofing your equipment from its biggest threat: Your end users.

Monkey: Anything that can go wrong, will go wrong.

Security Software

Software used to protect the system and other connected systems. LAPLACE is extensively fitted with information attack, countermeasure and defence software.

RedFROST

A customized version of the FROST Firewall v4.28, RedFROST leverages the unique AI elements of LA+ and its digital security and countermeasure systems in order to make intelligent defense decisions.

Viru-cide Red

Similar to RedFrost, Viru-cide Red is a varient of Awesome-corp's Viru-cide anti-viral/system diagnostic/active firewalling software with linkages to the unique AI elements of LA+ to further improve its functionality.

UMADS

UMADS(Universal Misuse and Anomaly Detection suite) is a false sandbox or 'honey comb' and experimental suite which fools an attacker into believing they have succeeded in penetrating a false computer - which only exists in emulation. At this point, an attacker usually stops, believing the system in question to lack any meaningful tactical potential as a target.

In this way, UMADS can be thought of as an electronic feign, to comprehend the enemy and their method of attack, identifying initial, primary, secondary and tertiary attacks. From here, any malware used in the attacking process is assessed in a 'zoo' (an emulated machine) and “ripples” in the code (ideal for performing buffer-overruns) are found: methods to get into the 'enemy' system.

Any attempt for an advanced attack to gain a foothold and ascend out of the emulated machine is met instantly with the emulated machine being nested inside another. This process can be continued indefinatey: inner nested computers disengaged – and should be thought of as trying to run up an escalator. This technique is known as a “Rabbit Hole” and succeeds at thwarting most forms of AI attacker.

An appropriate response is then issued as a 'flu-shot' as a list of security precautions and tests for other systems on the network to take - allowing for the beginnings of an attack response - all systems using LA+ acting as a single unified force in a return strike issued by ICE.

IIEDACS

IIEDACS (Information Intelligence Exchange Denial And Countermeasure System) excels in performing

advanced realtime ECM and information warfare operations: smearing enemy encryption codes, IFF, target information, prioritization information, communications and mission data beyond recognition: essentially denying the enemy's experts systems (such as PANTHEON) the very advantage XTAL offers. It is best used when tied to a starship grades communications and information processing system or in large numbers as part of a decentralized network, such as the Lazarus Communications network.

ICE

Intruder Countermeasure Electronics (ICE) is a means of formulating a return strike against an attacker. It contains a rich variety of modular malware and software and AI systems (including ROM constructs) which can be used to infiltrate an enemy system by disguising itself as legitimate traffic and then forcing variables in the end-system to move beyond storable variables into executable code (in what is known as a code injection or a malicious buffer-overrun).

Importantly is that ICE only works in a defensive fashion and requires information about its attacker before it can issue a strike.

- Tricking the enemy into attacking in a so called “false flag” attack is banned under the Terms of Use for LA+.

LEER

LEER (Low Event Emphasis System) acts as an additional decoder of live information coming in. Priority is placed not on 'brilliantly' suspicious systems but those with above-background level of anomaly but otherwise being entirely normal.

Detection thresholds force the system to only assess what combat detection systems would classically define as “low interest” objects.

LEER will then perform assessments using whatever sensor systems are available. In this way, low-interest and hidden objects which still produce emissions can be spotted without necessarily being blinded or ignored by the existence of traditionally high-interest systems.

OPSCURUS

Uses a construct as a cypher on obscuration. Necessary to connect to MOTHER.

APSTRUSUS

A live hardware encryption system, necessary to connect to and administrate a Lazarus node.