*Stichting NLnet phone:* XXX

Science Park 400 *e-mail:* [XXX](mailto:bureau@nlnet.nl)

1098 XH Amsterdam *XXX*

The Netherlands *XXX*

**Memorandum of Understanding**

*Number: 2024-04-415*

The parties:

**"*Slips Immune I*" Project**

and

**Stichting NLnet**, domiciled in Science Park 400, 1098 XH Amsterdam, The Netherlands, referred to as "**NLnet**" in this document, represented by **XXX**

given that:

**Czech Technical University in Prague**, Faculty of Electrical Engineering, an institution domiciled at Jugoslávských partyzánů 1580/3 160 00 Prague 6 - Dejvice in Czech Republic, represented by **XXX.**, referred to as "**CTU**" in this document

* **NLnet** has the mission *"to promote the exchange of electronic information and all that is related or beneficial to that purpose"*.
* **NLnet** manages the *NGI0 Commons Fund* fund, a fund dedicated to **open technologies** that **move the internet** and the **broader technology landscape** forward in terms of **privacy**, **resilience** and **trustworthiness**.
* **NLnet** collaborates with a number of other organisations and experts within *NGI0 Commons Fund* to help improve the quality, sustainability and adoption of projects in a structured way.
* Local networks are vulnerable to intrusions from bad actors. The existing tools for network monitoring and intrusion detection require a steep learning curve, and are not easily accessible to most users.
* CTU is a well-reputed organisation with ample experience designing new protocols and architecting and engineering software for intrusion detection. They work together with community members such as **XXX** and **XXX**

Inline substitution\_reference start-string without end-string.

* **CTU** by means of **XXX** has devised a plan that can contribute to creating Slips Immune, an "Internet Immune System". By implementing an AI powered Intrusion detection and prevention system on a Raspberry Pi for advanced detection and blocking, and integrating it with a LLM to improve decision making and summarization, they bring network monitoring and protection to everyone.
* **CTU** wants to work on the above ideas in the public interest, and intends to deliver the results not as proprietary solutions, but as free and open source building blocks that anyone can download for free, and that within the open license chosen grant any person or organisation the right to use and repurpose part or whole without restrictions - including the right to modify every functional aspect in order to serve their own particular needs and the needs of others.
* **NLnet** thinks that this project falls within its mission and the mission of the *NGI0 Commons Fund* fund, and wants to facilitate such a contribution.

agree to the following:

1. On behalf of **CTU**, **XXX** has written the proposal "*Slips Immune I*" which is attached to this document as Annexe I. Annexe I forms an integral part of this Memorandum of Understanding. If and where statements in this annexe or other annexes are in contradiction with one or more statements in the main memorandum text, the statement or statements in the main memorandum text will prevail.
2. **CTU** is voluntarily undertaking the project, and is solely responsible for all aspects of the project including planning and coordination as well as involving contributors and partners - as long as such happens in line with the terms and spirit of this MoU, and with their explicit and voluntarily consent to join this Memorandum of Understanding with all its stated obligations and provisions, and to act in good faith.
3. The source code and technical designs of the Project (as well as any documentation and supporting materials officially produced within the project) are to be made openly available to the general public under a suitable free/libre/open source software or hardware license. Eligible licenses include the licenses recognised by OSI and FSF.
4. **XXX.** shall act as signatory on behalf of **CTU**, and confirms to be mandated to act as official point of contact in the context of this project; it is the responsibility of **XXX** to notify **NLnet** in case of any changes or issues.
5. **NLnet** commits to make a reservation for the amount of **16280** EUR to **CTU** in order to support the "*Slips Immune I*" project. The reservation is bound to the proposal as contained within *Annexe I* of this MoU.
6. Should the project fail to complete the goals described in Annexe I, partially or in full, there is no other consequence than the termination of this MoU.
7. **CTU** commits to keep the user and developer community up to date with progress made within the project at least every two months (more often is never a bad thing) and will maintain a public status page for the project to keep the wider internet community informed. As a courtesy, **CTU** may send non-public updates about the status of the project to **NLnet**, but there is no obligation whatsoever to do so - **NLnet** is not operationally involved with the project; its only interest is the public benefit that is the result of the project succeeding in reaching its goals. **CTU** commits to help NLnet to clear any uncertainties about the overall effort and project achievements should the need for that emerge (e.g. in the context of an official audit).
8. The validity of the Memorandum of Understanding is one calendar year (twelve months) from the date of signing. If the project is not finished at this point of expiry, and the work is still relevant, it may be prolonged based on mutual agreement between **NLnet** and **CTU**. Any *amendment* to the MoU only changes the validity period if it explicitly establishes a new time frame, otherwise the original validity period stays intact.
9. Donations may be claimed up to the reserved amount within the validity of the (amended) Memorandum of Understanding. Donations will be final when the specified milestones or previously agreed partial deliveries have been verified to have been completed. Payments will subsequently be made by wire transfer into bank account IBAN CZ1201000001071700230207 / SWIFT Code / BIC: KOMBCZPPXXX. Payment requests submitted at a later date are not guaranteed to be paid.
10. **NLnet** and **CTU** may issue one or more individual or joint public statements announcing the project and the financial support from **NLnet** and the *NGI0 Commons Fund* fund. **CTU** is also encouraged to visibly and vocally acknowledge this contribution and the contribution of EC to the *NGI0 Commons Fund* fund [1](#_bookmark2) where possible — e.g. through the public world wide web, promotional materials, in presentations, in the credits section of software and in source code.
11. All parties commit to adhere to the IEEE Code of Ethics. [2](#_bookmark3) The involvement with any particular person(s) or organisations will be on the understanding that these coordinate their activities in agreement with **XXX**, in the spirit of cooperation, and in an effort to achieve the results of the "*Slips Immune I*" project. **CTU** appreciates the support from the experts and organisations involved with *NGI0 Commons Fund* to ensure that the results of *Slips Immune I* will be of the widest possible benefit to all.
12. This Memorandum of Understanding cannot be seen as any kind of employment
13. The NGI Zero Commons fund was established with financial support from the European Commission's **Next Generation Internet** programme, under the aegis of DG Communications Networks, Content and Technology under grant agreement No 101092990, under the aegis of *DG Communications Networks, Content and Technology*.
14. IEEE Code of Ethics, see: https://[www.ieee.org/about/ethics](http://www.ieee.org/about/ethics)

agreement or business contract. **NLnet** nor any of the organisations involved with *NGI0 Commons Fund* receive any goods or services as a result of this MoU. Any payments are to be made as charitable donations to **CTU** in the light of a voluntary contribution to the public benefit such as defined within the statutory mission of **NLnet foundation**. **CTU** is responsible for paying any and all taxes or other fees with regard to this grant, should there be any, and to inform any relevant authorities within their country of these donations should this be legally required.

On behalf of **NLnet** On behalf of **Czech Technical University in Prague**

**XXX XXX**

(Place) (Date) (Place) (Date)

**Annexe I: Project plan *Slips Immune I***

Slips Immune I is the initial step toward developing an Internet Immune System, which aims to protect connected devices through decentralized P2P technology by enabling them to share and respond to attacks collaboratively. The project focuses on implementing an Intrusion Detection/Prevention System (IDS/IPS) on Raspberry Pi devices with advanced detection and blocking capabilities, such as ARP poisoning and firewall protection. It also incorporates machine learning tools like TensorFlow and Torch for enhancing attack detection. The second part of the project explores integrating Large Language Models (LLM) to improve decision-making, evidence summarization, and flow classification in network security tasks. The outcomes include free software tools, a new isolation module, and a fine-tuned LLM for enhanced cybersecurity functions.

# A1: Research Limitations

Update and test the research limitations due to the current hardware, llm models and capabilities. Evaluate the limitations of the latest Rpi in quantized models. Decide on threshold and performance that can be expected.

# Milestone(s)

* 1. Evaluate Raspberry Pi's processing limitations and define acceptable performance benchmarks. (€ 822)
  2. Specify the minimum software and hardware requirements. (€ 823)

# Amount

€ 1645

# A2: RPI Compatibility

Implementation and adaptation of Slips to the Rpi architecture. From ARM architecture to memory management. Also storage of files, logs, outputs, models, etc. After this stage Slips should minimally run in Rpi.

# Milestone(s)

* 1. Re-implement SLIPS features incompatible with Raspberry Pi. (€ 1645)

# Amount

€ 1645

# A3: Develop SLIPS Light Version for Raspberry Pi

Slips uses many large libraries and models (tensorflow, torch) that require gigabytes of storage and memory. After Slips is running, prune and cut and migrate to lightweight versions of these libraries and features, to have a Slips that not only runs but is fast and nimble in the Rpi.

# Milestone(s)

* 1. Create a lightweight version of SLIPS optimized for Raspberry Pi. (€ 1645)

# Amount

€ 1645

**4. A4: Network Blocking and Unblocking Mechanisms with ARP Poisoning**

Network blocking and unblocking are paramount for the operation. Desing how and when this will be used with ARP poisoning. Create the mechanisms for IP tracking to see how is blocked, and the timing criteria.

# Milestone(s)

1. Design a mechanism using ARP poisoning to block attackers within the network. (€ 822)
2. Define criteria and timing for unblocking attackers, including tracking blocked IPs. (€ 823)

# Amount

€ 1645

# A5: ARP Poisoning Security Measures

ARP poison is considered an attack. We need to announce the instance of slips doing the attack to avoid detecting it as an attacker by other Slips in the network. And add measurements to avoid accidental blocking of benign hosts.

# Milestone(s)

* 1. Ensure all SLIPS instances in the network are aware of the blocking Raspberry Pi instance via ARP poisoning to avoid blocking it. (€ 822)
  2. Research possible risks of ARP poisoning (like accidental blocking or network disruptions) and implement fail-safes to minimize impact (€ 823)

# Amount

€ 1645

# A6: IDS-in-the-Middle Blocking with iptables

Make sure Slips and the raspberry PI can be in the middle of the router and the hosts filtering out malicious actors for the entire network using iptables.

# Milestone(s)

* 1. Implement an IDS-in-the-middle setup using iptables to prevent network clients from accessing harmful sites. (€ 1645)

# Amount

€ 1645

# A7: IDS-in-the-Middle Traffic Routing

An IDS-in-the-middle functions as a transparent bridge that inspects network traffic without altering its flow. Like a proxy. Make sure slips can route traffic from both Ethernet and Wifi connections from the router to the clients.

# Milestone(s)

* 1. Implement IDS-in-the-middle traffic routing over both Ethernet and WiFi connections. (€ 1645)

**Amount**

€ 1645

**8. A8: Routing Failover**

Set up a failover mechanism to preserve network connectivity if the Raspberry Pi goes down. (e.g., an alternative gateway or bypass method).

**Milestone(s)**

a. Implement a failover mechanism to maintain network connectivity if the Raspberry Pi fails (€ 1645)

**Amount**

€ 1645

**9. A9: Performance Evaluation and Validation**

Setup a testing environment, and start capturing traffic in all of them with Slips in-the middle between them and the router, and test how Slips (The instance of Slips in the RPI acting as the immune system) behaves in terms of RAM, CPU usage, Disk usage, Heating, etc.

**Milestone(s)**

1. Conduct real-life performance evaluations by testing SLIPS on Raspberry Pi in real-life scenarios with three to four computers. (€ 822)
2. Measure detection speed and efficiency. (€ 823)

**Amount**

€ 1645

**10. A10: Testing**

Stress testing and Pinpoint weak points; Latency, flow and evidence timing issues, reliability, integration problems, etc.

**Milestone(s)**

1. Set up the testing environment, including mock network traffic generation. (€ 822)
2. Pinpoint weak points; Timing issues, Failover reliability, integration problems, etc. (€ 823)

**Amount**

€ 1645

**11. A11: Performance improvements**

Fix the issues discovered in the Testing (A10) and Performance Evaluation and Validation (A9) phases .

**Milestone(s)**

a. Fixes of the issues discovered in the evaluation and testing phases. (€ 1645)

# Amount

€ 1645

# A12: Maintenance and Documentation

Implement and improve logging with log rotation to for Slips/zeek log files to prevent them from consuming too much disk space. and document experiments, setup, requirements, installations, how to use, limitations, future improvements, and benchmarks.

# Milestone(s)

* 1. Implement logging and log rotation for key events (e.g., detections, blocked/unblocked IPs) to aid in troubleshooting and performance review. (€ 822)
  2. Document installations, limitations, benchmarks, and experiments. (€ 823)

# Amount

€ 1645

# B1: LLM Research and Selection

Analyze and evaluate the latest LLMs for small-device viability. Use a minimal evaluation framework ( probably based on promptfoo) to methodically evaluate summary, decision making and tool usage performance on SLIPS-like scenarios, ensuring adaptability to rapid innovation. Consider function calling viability in the baseline models.

# Milestone(s)

* 1. Survey LLM models to use and fine-tune in small devices. Pay special attention to models with open-source-compatible licenses. (€ 500)
  2. Create a minimal setup for evaluating the LLM performance applied to decision-making and flow interpretation in a context similar to SLIPS. (€ 500)

# Amount

€ 1000

# B2: LLM performance on RPi

Examine LLM performance on the Raspberry Pi 5 architecture, emphasizing CPU, memory, and storage constraints. Explore different inference frameworks to determine viable deployment under hardware limitations.

# Milestone(s)

* 1. Measure the performance of the selected model in Rpi in terms of tokens/s, CPU usage, Memory, etc. (€ 500)
  2. Evaluate the performance of different inference frameworks (€ 500)

# Amount

€ 1000

# B3: Dataset Creation for flow analysis and summarization

Adapt the selected model for the SLIPS context by fine-tuning on a dataset containing alerts and relevant information of the flow, ensuring the correct output format. This approach is preferred over extended context usage to speed up inference and reduce token processing overhead.

# Milestone(s)

* 1. Develop a dataset tailored for fine-tuning models, focusing on flow summarization and analysis with an emphasis on applications in small device environments. (€ 500)
  2. Improve the dataset by incorporating labels generated through human annotation and advanced LLMs. (€ 500)

# Amount

€ 1000

# B4: Dataset creation for decision making.

Create a new dataset of alerts and preferred actions, starting with SLIPS outputs and human preprocessing. Augment this dataset using insights from larger LLMs to enhance coverage and accuracy.

# Milestone(s)

* 1. Create a dataset for the fine-tuning process considering the context of small devices in decision making in network security. (€ 500)
  2. Improve the dataset by incorporating labels generated through human annotation and advanced LLMs. (€ 500)

# Amount

€ 1000

# B5: Fine Tuning setup

Evaluate available frameworks for fine-tuning the chosen model, then implement the required scripts on x64 architecture and NVIDIA GPU-based training.

# Milestone(s)

* 1. Research possible frameworks for fine-tuning LLM, considering speed and model performance. (€ 500)
  2. Develop the scripts and code necessary for conducting the fine-tuning on x64 architecture and NVIDIA GPU (€ 500)

# Amount

€ 1000

# B6: Preliminar fine tuning and Model Evaluation for flow analysis

Evaluate the fine-tuned model against the baseline by extending the initial promptfoo-based evaluation framework. Add new test cases that focus on flow analysis and summarization to thoroughly compare performance.

# Milestone(s)

* 1. Evaluate the fine-tuned model for flow analysis considering the performance of the vanilla model (€ 500)
  2. Extend the evaluation framework for considering flow analysis and summary. (€ 500)

# Amount

€ 1000

# B7: Preliminar fine tuning Model Evaluation for decision making

Evaluate the fine-tuned model against the baseline by extending the initial promptfoo-based evaluation framework. Add new test cases that focus on flow analysis and decision-making to thoroughly compare performance.

# Milestone(s)

* 1. Evaluate the fine-tuned model for decision making considering the performance of the vanilla model. (€ 500)
  2. Extend the evaluation framework for considering the decision process inside SLIPS. (€ 500)

# Amount

€ 1000

# B8: Merge models viability

Adapt the scripts to fine-tune the selected model using both datasets, aiming for a single model that handles summary, flow analysis, and decision-making. Evaluate the performance in terms of resource usage and result quality. Compare the results with the performance of individual models.

# Milestone(s)

* 1. Evaluate the viability of fine tuning just one model for flow analysis and decision making. Performance, computer resources. (€ 500)
  2. Implement and evaluate possible strategies for using both models in parallel. (€ 500)

# Amount

€ 1000

# B9: Quantization

Apply and evaluate various quantization approaches to enhance speed and reduce resource usage. Compare these quantized models against their unquantized counterparts, focusing on both computational efficiency and output quality

# Milestone(s)

* 1. Apply different quantization approaches to improve the inference speed of the models. (€ 500)
  2. Evaluate the performance loss of the quantized models. (€ 500)

**Amount**

€ 1000

**22. B10: Model Evaluation**

Conduct a thorough evaluation using new, real-life SLIPS data and produce a detailed report of the results.

**Milestone(s)**

1. Evaluate the fine-tuned and quantized model for flow analysis and taking security decisions based on real-life information provided by SLIPS . (€ 500)
2. Write a detailed report with the results (€ 500)

**Amount**

€ 1000

**23. B11: Calling SLIPS tool for blocking**

Implement function-calling in the model to enable actual blocking actions rather than merely describing them. Evaluate the results to ensure correct and effective execution.

**Milestone(s)**

1. Adapt the the LLM for calling SLIPS tool for blocking a host (€ 500)
2. Evaluate model capabilities for calling SLIPS tool (€ 500)

**Amount**

€ 1000

**24. B12: Maintenance and Documentation**

Produce the documents describing the whole fine-tuning process and model deployment. Documentation should provide all the necessary information for replicability. Include possible approaches for updating the model to adapt to new threads (new finetuning or simply add new context if possible)

**Milestone(s)**

1. Analize possible maintenance and update strategies for the LLM model to adapt to new threats. (€ 500)
2. Document the fine-tuning process and model deployment. (€ 500)

**Amount**

€ 1000

**25. C1: Architectural Design for the New Version of SLIPS Including LLM**

Develop a comprehensive architectural design for the next version of SLIPS, incorporating the integration of a large language model.

**Milestone(s)**

a. Design documented (€ 2180)

**Amount**

€ 2180

**26. C2: Implement the Decision Model and Summary Feature in SLIPS**

Develop and integrate a decision-making model into SLIPS, along with a summarization feature to generate concise insights.

**Milestone(s)**

a. Decision model of summary published and documented (€ 2000)

**Amount**

€ 2000

**27. C3: Conduct Stress Testing for SLIPS Infrastructure**

Develop a framework to simulate high-traffic scenarios and test SLIPS's performance under stress.

**Milestone(s)**

a. Documentation on tests published with results (€ 2000)

**Amount**

€ 2000

**28. C4: Evaluate the Decision Model and Summary Feature in SLIPS**

Conduct a comprehensive evaluation of the decision model and summarization feature, including performance testing and feedback.

**Milestone(s)**

a. Evaluation implemented, tested and documented. (€ 2000)

**Amount**

€ 2000

**29. C5: Design and Implement an Update Functionality for SLIPS**

Develop two secure and reliable update mechanisms for SLIPS, including authentication and fallback systems.

**Milestone(s)**

1. Add support for manual updates where slips only updates when the user stops it and manually updates it. (€ 1000)
2. Implement reliable automatic live-update where slips updates to the new version while

running without user interaction. Runs only when allowed by the user in the configuration file. (€ 1000)

**Amount**

€ 2000

**30. C6: Document and Publish Results from SLIPS Improvements**

Improve and document the Raspberry Pi-specific version of SLIPS and publish a research article summarizing the results.

**Milestone(s)**

a. Documentation published (€ 2000)

**Amount**

€ 2000

**31. C7: Architectural Immunity Model Design**

Design of Immunity models on Slips, which ones we will do first, which is the priority and dependencies. Elaborate on each model and document why we are choosing it.

**Milestone(s)**

a. Design documented and published (€ 2000)

**Amount**

€ 2000

**32. C8: Immune idea 1: Automatically creating AD models and Training on benign detections**

Immune idea 1 to implement: Automatically creating Anomaly Detection (AD) models and Training on benign detections. This means implementing many techniques and testing

**Milestone(s)**

a. Development done and published (€ 1000)

**Amount**

€ 1000

**33. C9: Immune idea 2: Automatic threshold adaptation. Risk levels**

Immune idea 2: Automatic threshold adaptation. The majority of the systems do not handle risk levels, or risk states, similar to the DEFCON standard. Design, test and create the adaptive risk levels for threshold management.

**Milestone(s)**

a. Development done and published (€ 1000)

# Amount

€ 1000

**34. C10: Immune Idea 3: Selection of different detection methods for different risk levels**

Selection of different detection methods for different risk levels. Each predefined risk level has to have its own detection methods and thresholds. More importantly it has dependencies and 'activations' from other parts of the system.

# Milestone(s)

a. Development done and published (€ 1000)

# Amount

€ 1000

# C11: Immune Idea 4: Innate and adaptive Immune system

Separate the Innate and adaptive Immune system. In most IDS tools there is no concept of innate system that works as a first layer of protection and is fast to act. Nor they have a second system that is harder to activate but very very powerful. Study them and implement.

# Milestone(s)

* 1. Development done and published (€ 500)

# Amount

€ 500

# C12: Evaluation of results of external security audit

This task is to evaluate the results of the external audit, see how to fix the issues found, and publish the fixed version

# Milestone(s)

* 1. Document with evaluation of results (€ 500)

# Amount

€ 500