Official M1 Milestone Course Submission Report V1.0

Project: Wallet–RPC Privacy Leakage Measurement (Empirical Study)

Course: CS6290Version: V1.0 (Formal Submission Version)

1. Project Overview & M1 Milestone Core Objectives

1.1 Project Positioning

This project is an empirical study focusing on privacy leakage risks in the Wallet-RPC interaction scenario of Ethereum. It aims to build a configurable, reproducible, and privacy-first measurement framework to quantify the privacy exposure, service availability, and performance characteristics of mainstream RPC service providers, and systematically identify potential privacy leakage attack vectors in the RPC interaction process.

1.2 M1 Milestone Non-negotiable Core Objectives

All objectives are fully aligned with CS6290 course requirements and project phased planning, with no out-of-scope design:

1. Complete the full-module development of the baseline RPC privacy measurement harness, realizing the end-to-end closed loop of automated experiment execution, desensitized data logging, and verifiable metric calculation.
2. Complete the baseline functional verification experiment on the Ethereum Sepolia testnet, confirm the correctness, stability, and observability of the measurement framework, and output verifiable experimental results.
3. Establish a unified project governance system, including full-cycle

achievement archiving specifications, standardized repository structure, and clear 5-person team role division, to support subsequent milestone iterations.

4. Complete the theoretical framework and visualization system design of the empirical study, including threat model construction, privacy measurement dimension definition, and core data flow sorting.

5. Complete all mandatory compliance deliverables required by the CS6290 course, including individual evidence packs, AI usage transparency disclosure, and reproducible experiment resources.

2. Full Completed Deliverables & Achievements of M1 Phase

All content in this section is based on actual submitted project files, with corresponding source files for each achievement, no fiction or assumption, and no repeated detailed content of existing archiving specification and visualization package documents.

2.1 Full-Module Development of Config-Driven RPC Privacy Measurement Harness

We have completed the end-to-end development of the Python-based measurement harness, the core infrastructure of this empirical study. 5 core functional modules are fully implemented, with all codes archived in the src/ directory of the project repository:

· **JSON-RPC Client Module (rpc_client.py)**: Encapsulates the underlying request client with timeout control, proxy support, and full exception capture capabilities. It realizes full lifecycle management of RPC request sending, latency statistics, response parsing, and error marking, providing stable underlying request support for the entire measurement process.

· **Scenario Execution Engine (runner.py)**: Implements a fully config-driven automated experiment execution process. It supports loading YAML configuration files via environment variables, automatically matches preset experiment scenarios,

executes requests cyclically according to the set duration and interval, and automatically generates timestamped log files, realizing one-click execution and 100% reproducibility of experiments.

· **Privacy-First Structured Logging Module (logger.py):** Implements desensitized log recording that meets privacy measurement requirements. Core functions include: SHA256 hashing of request parameters to replace raw parameter storage, avoiding sensitive data retention; heuristic Ethereum address detection to mark the has_address field, providing the core identifier for privacy exposure measurement. It supports append writing of JSONL format logs, fully compatible with downstream data analysis.

· **Extensible Scenario Definition Module (scenarios.py):** Standardizes the encapsulation of scenario-based RPC requests. 4 core scenarios are predefined in the M1 phase: address-free baseline scenario blocknumber, address-bearing privacy scenarios balance and nonce, and basic call scenario. All scenarios return standardized (method, params) tuples, supporting flexible expansion in subsequent milestones.

· **Automated Metric Summarization Module (summarize.py)**: Implements one-click calculation of verifiable measurement metrics from raw JSONL logs. Core statistical dimensions include total requests, success/error rate, latency statistics (mean, median, min, max), address-bearing request ratio, scenario/method distribution, and error type statistics. It supports batch analysis of multiple log files, providing core quantitative capabilities for A/B comparison of RPC providers.

2.2 Reproducible Experiment Configuration & Standardized Test Resources

We have completed the preparation of standardized experiment configuration files and compliant test resources, ensuring all team members can reproduce the M1 baseline experiment without modifying the code:

1. **Dual-Provider Standard Experiment Configurations:** Completed 2 sets of

YAML configuration files for the Sepolia testnet (exp_sepolia_providerA.yaml, exp_sepolia_providerB.yaml), corresponding to two mainstream RPC service providers. The configuration covers provider ID, chain ID, RPC endpoint, experiment scenario, address file path, execution duration, request interval, and log output path, realizing unified management of experiment parameters.

2. **Compliant Test Address Resource**: Provided a standardized demo address file (addresses_demo.txt), using only the Ethereum testnet demo address, no real user sensitive wallet address, fully complying with the project's privacy desensitization requirements.

2.3 Project Governance & Full-Cycle Achievement Archiving System

We have completed the formulation and implementation of the Full-cycle Project Achievement Archiving Specification V1.0, establishing a unified standard for team collaboration and achievement management throughout the project lifecycle:

1. Defined 5 core archiving principles (reproducibility & verifiability, course compliance first, iterative compatibility, secure desensitization, unified collaboration) as the bottom-line rules for project delivery.

2. Designed a standardized 7-directory GitHub repository framework, fully compatible with the existing project structure, clarifying the core archiving purpose of each first-level directory, while retaining the flexibility of subdirectory adjustment for each role.

3. Formulated milestone-based archiving rules, clarifying the mandatory archiving content for M1, M2, and M3 milestones, avoiding delivery omissions in subsequent iterations.

4. Set 4 mandatory compliance rules and a pre-submission validation checklist, ensuring all project deliverables fully meet CS6290 course requirements.

5. Clarified the full-process archiving responsibilities of 5 core team roles, with clear boundaries and no overlap, matching the individual evidence pack submission requirements of the course.

2.4 Empirical Study Theoretical Framework & Visualization System

We have completed the design of the M1 milestone visualization package and the construction of the core theoretical framework of the empirical study, providing theoretical support and standardized display for the project:

1. Clarified the core boundaries and scope of the M1 phase, explicitly defining the implemented measurement scenarios and out-of-scope expansion directions, avoiding scope creep and forming a unified team consensus.
2. Built a layered privacy leakage threat model for the Wallet-RPC scenario, sorting out the complete attack chain from attacker entities to attack vectors and final privacy risks, providing threat-driven logical support for the design of measurement indicators.
3. Drawn the core data flow diagram of the M1 measurement framework, presenting the full data flow from configuration input to result output, clarifying the responsibilities of each module, and forming a unified process consensus for team development and experiment execution.
4. Defined 3 core measurement dimensions (availability, performance, privacy exposure) and their corresponding proxy indicators, all of which can be directly collected and calculated by the developed measurement framework, realizing the one-to-one mapping of "threat model - measurement indicator - experimental collection".

2.5 Course Mandatory Compliance Deliverables

We have completed all mandatory compliance deliverables required by the CS6290 course:

1. Completed the Individual Evidence Pack (Milestone 1) for the Developer / Tool Developer role, which records personal contributions, verifiable evidence links, full experiment validation process, and AI usage transparency disclosure in detail.
2. Established a unified archiving framework for AI usage transparency records

of all team members, clarifying mandatory disclosure requirements, fully meeting the course's AI collaboration transparency rules.

3. Completed desensitization of all project deliverables, no unmasked sensitive data (private RPC URLs, real wallet addresses, private keys) is included in the public repository, complying with data security requirements.

3. Baseline Experiment Execution & Validation Results

All experiment processes and results are fully consistent with the actual execution records in the individual evidence pack, with a complete verification process and traceable results.

3.1 Experiment Setup

Target Network: Ethereum Sepolia Testnet

Measurement Objects: 2 mainstream RPC service providers (Provider A: Public Node, Provider B: Tenderly Gateway)

Core Validation Scenario: Address-bearing privacy scenario eth_getBalance (core scenario for privacy leakage measurement)

Control Variables: Fixed test address, consistent chain environment, controlled execution duration and request interval for each provider

Core Validation Dimensions: Request correctness, connectivity, error handling capability, metric integrity

3.2 Full Validation Process

1. Executed the measurement harness with standard configuration files of Provider A and Provider B respectively in the Sepolia testnet environment, and generated structured JSONL logs for each experiment.

2. Used the summarize.py script to calculate the core metrics of the logs, and verified the consistency between the statistical results and the experiment configuration.

3. Verified the correctness of core RPC methods: confirmed that the eth_getBalance

method correctly marked has_address=true, and the eth_blockNumber method correctly marked has_address=false.

4. Verified the observability of error handling: confirmed that abnormal requests can be correctly marked with status=error and recorded with clear error reasons.

5. Verified the integrity of the metrics: confirmed that the total number of requests, scenario/method distribution, and address-bearing ratio in the summary results are completely consistent with the preset experiment configuration.

3.3 Final Experiment Results

1. **Functional Correctness:** All requests of the balance scenario for both providers were executed successfully, with a 100% request success rate (ok_rate=1.000), no timeout or HTTP exceptions occurred in the baseline experiment.

2. **Framework Stability:** The measurement framework ran stably throughout the experiment, with complete log fields, correct parameter hashing, and accurate address detection, no program exceptions or data loss occurred.

3. **Metric Verifiability:** All statistical metrics output by the summarization script are completely consistent with the experiment configuration and raw log data, and the results are fully traceable and reproducible.

4. **Objective Limitation Statement:** The M1 baseline experiment only completed short-duration and low-request-volume tests. Endpoint instability (timeout, rate limiting) under long-duration, high-concurrency scenarios will be systematically evaluated in the M2 milestone.

4. Team Role Division & Corresponding Deliverables

Fully aligned with the 5 core roles defined in the archiving specification, the corresponding deliverables of each role in the M1 phase are as follows:

Role	Core Responsibilities in M1	Corresponding Completed Deliverables
Project Management & Archiving Lead	Specification maintenance, repository compliance review, milestone progress coordination, delivery integrity assurance	Full-cycle Project Achievement Archiving Specification V1.0, pre-submission validation checklist, team role division system
Developer / Tool Developer	Core measurement harness development, experiment configuration preparation, experiment execution & validation, code repository maintenance	Full 5-module measurement harness code, standard experiment configuration files, individual evidence pack, experiment validation results
Document & Specification Lead	Project document archiving, milestone report compilation, presentation material production	M1 milestone submission report, presentation slides, standardized document archiving system
Security & Threat Model Lead	Threat model construction, privacy risk sorting, validation scheme design, result cross-verification	Layered privacy leakage threat model, experiment validation scheme, measurement dimension-threat mapping table
Research & Data Analysis Lead	Pre-research literature sorting, measurement indicator design, data analysis framework design, visualization system construction	Milestone Presentation Visualization Package V1.0, 3 core measurement dimensions and proxy indicator system, data flow diagram

Role	Core Responsibilities in M1	Corresponding Completed Deliverables
All Team Members	Comply with archiving specifications, submit individual evidence packs, complete AI usage transparency disclosure	Personal work archiving, AI usage records, individual evidence packs for each milestone

5. M1 Milestone Overall Progress Achievement

All preset core objectives of the M1 milestone have been 100% completed, no overdue content, no out-of-scope design, all deliverables are based on actual implementation:

1. **Core Tool Development Goal 100% Achieved:** Completed the full-module development of the config-driven RPC privacy measurement harness, realizing the end-to-end closed loop of request execution, desensitized logging, and metric summarization. The tool can run stably and the baseline experiment is fully reproducible.
2. **Experiment Validation Goal 100% Achieved:** Completed the baseline scenario experiment of two RPC providers on the Sepolia testnet, completed the full-dimensional verification of the framework's correctness, stability, observability, and metric integrity, and the experimental results meet expectations.
3. **Project Governance Goal 100% Achieved:** Completed the formulation of the full-cycle archiving specification, standardized repository framework, and clear team role division, providing a complete collaboration standard for subsequent milestone iterations.
4. **Theoretical Framework Goal 100% Achieved:** Completed the construction of the threat model, measurement dimension system, and visualization framework,

providing solid theoretical support for the subsequent empirical study.

5. **Course Compliance Goal 100% Achieved:** Completed all mandatory compliance deliverables required by the CS6290 course, fully meeting the course's scoring rules and submission requirements.

6. M2 Milestone Follow-up Plan

Based on the M1 phase achievements, the core work of the M2 milestone is planned as follows, no out-of-scope design:

1. Expand experiment scenarios, cover more RPC methods and privacy-related interaction scenarios, and enrich the measurement dimensions of privacy exposure.
2. Expand the scale of the experiment, increase the number of measured RPC providers, extend the experiment duration, increase request concurrency, and systematically evaluate the stability and privacy leakage risks of providers under real workloads.
3. Optimize the threat model and measurement indicator system, refine the quantitative method of privacy leakage, and improve the academic rigor of the empirical study.
4. Complete mid-term experimental data analysis, output phased empirical research conclusions, and complete the M2 milestone team report and individual evidence packs for all team members.