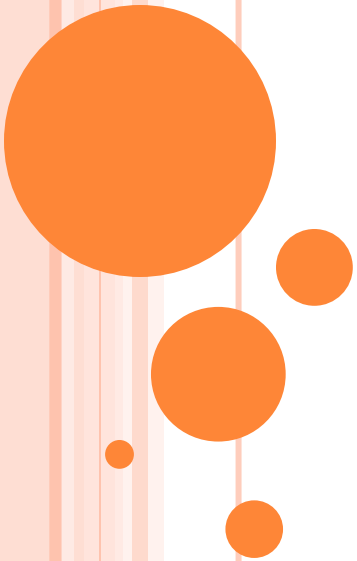


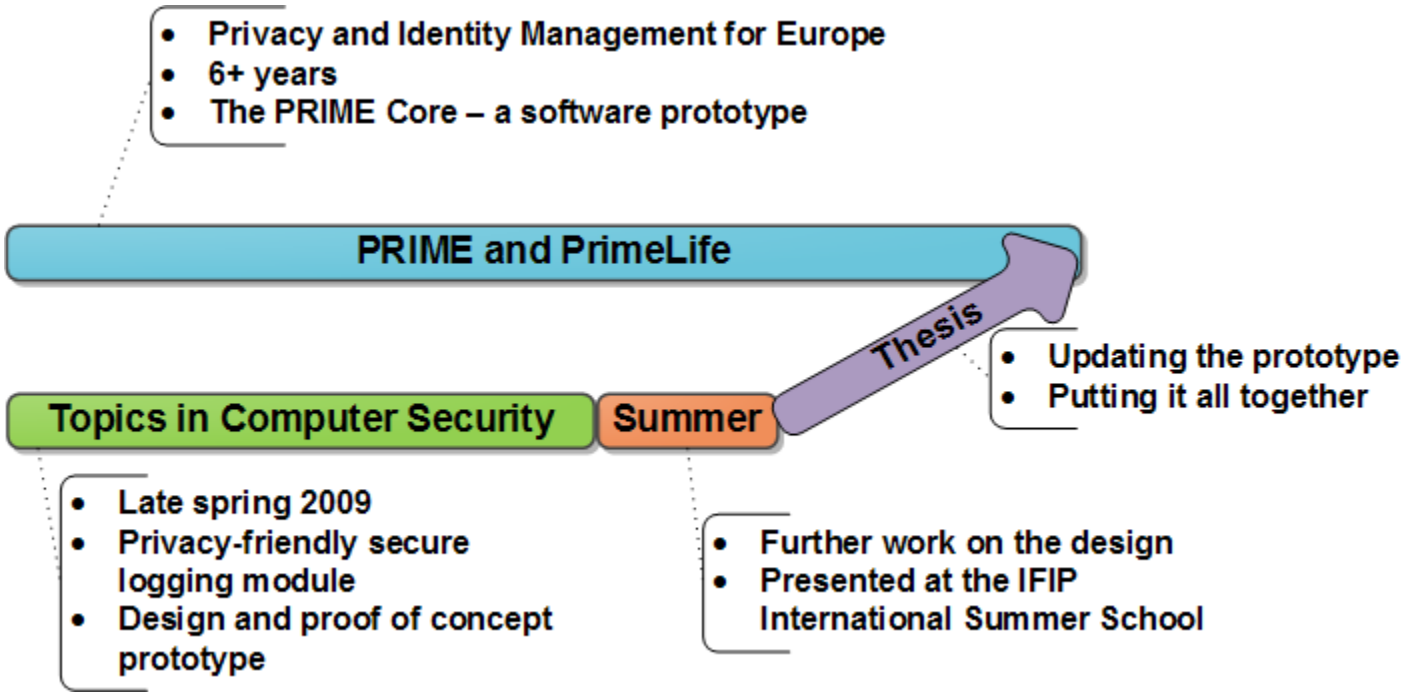
# Implementing a Privacy-Friendly Secure Logging Module into the PRIME Core

Anders Ellvin, Tobias Pulls

# Introduction

- Background and the assignment
  - Implementing a privacy-friendly secure logging module into the PRIME Core
- What is the PRIME Core and PrimeLife
- What is a privacy-friendly secure log
- Our work – three milestones
- Evaluation and future work

# Background & Assignment



# A Privacy-Friendly Secure Log

- **Secure** Log
  - Protects the confidentiality and integrity of entries
  - Prior to an attacker compromising the log
- **Privacy-Friendly** Secure Log
  - Only the data subject can decrypt the entries belonging to him or her
  - A high degree of unlinkability between log entries and data subjects

# Milestone 1

- Naming and coding conventions
- Centralized configuration
- Creating the KeyHandler
- The EventSelector
- Log Integrity Validation
- Junit Tests

# Milestone 2 - API

- Java Web Services
  - SOAP messages
  - How client and server PRIME Cores communicate
- GetLogEntry(EntryID)
  - Returns the entry with the given ID
- GetLatestEntryID(subject)
  - Returns the latest EntryID for the data subject

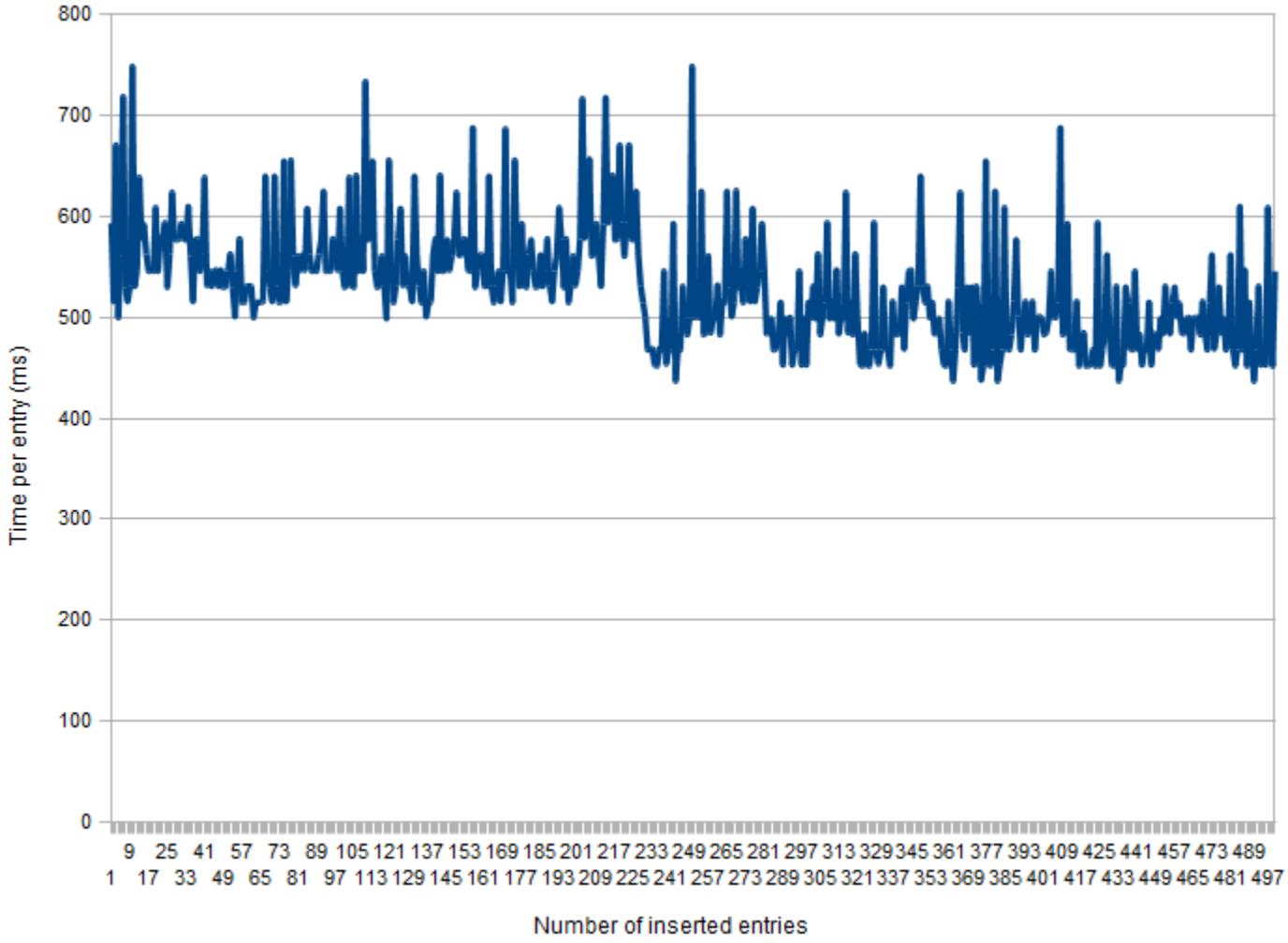
# Milestone 2 – Sharing Secrets

- All the security and privacy properties ultimately comes from secrets
  - Needed for the server and each data subject
    - Validation of their respective log entries
- Server secrets => start of the PRIME Core
  - Two values and a keypair
  - Dumped to file using PBE and then discarded
- Data subject secrets => at the disclosure of PII
  - For each data subject: two values and a public key to the server, the private key remains secret
  - Generated client-side

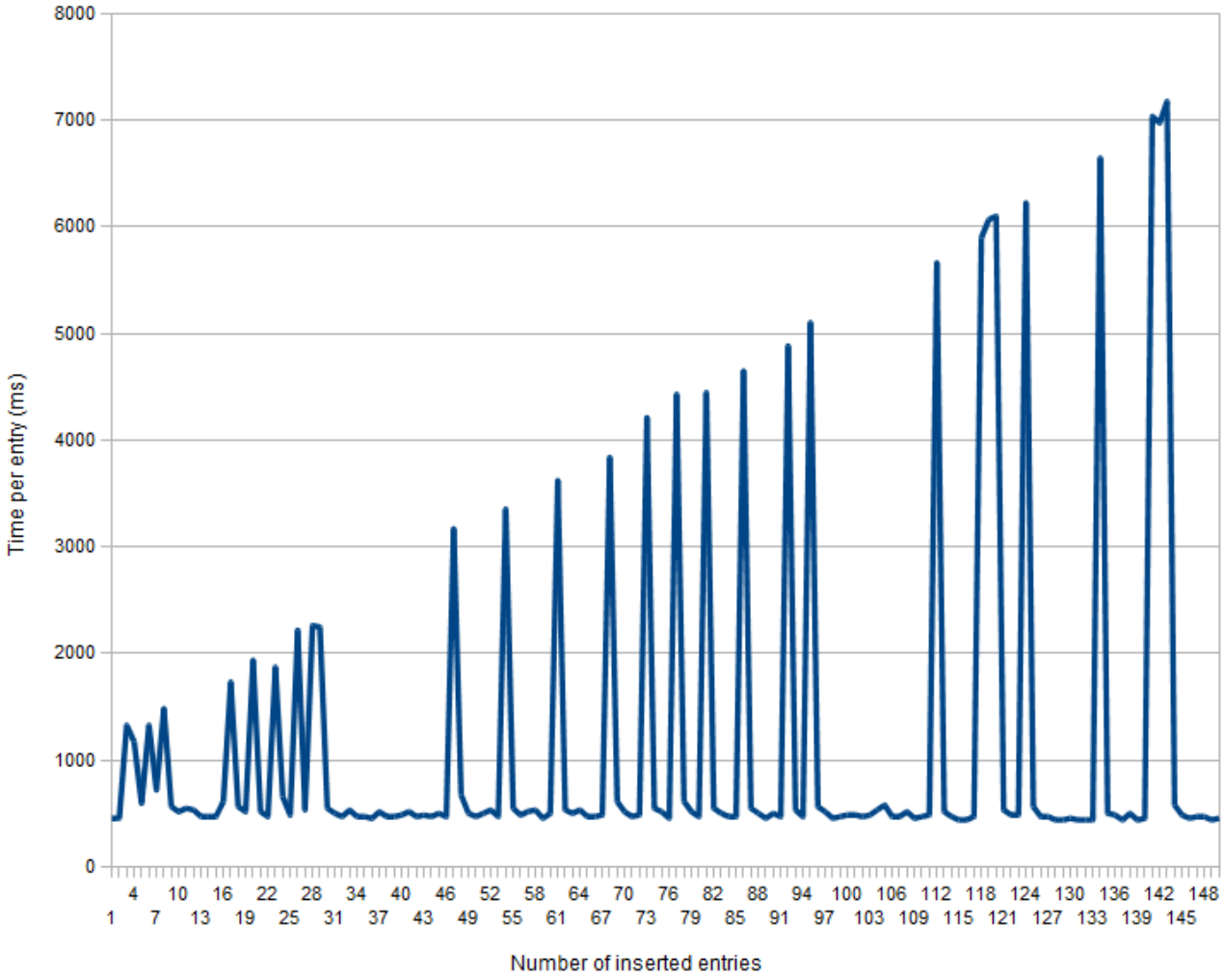
# Milestone 3 - HSQLDB

- HSQLDB is a database written in Java
- Order of entries in the log + correlation with other source => privacy problem
- Several table types, only text suitable
- Mitigation developed, the Shuffler
  - Data inserted => chance to trigger a shuffle
  - Disconnect the table, shuffle and then reconnect
- Lacking performance

# Shuffler Performance – turned off



# Shuffler Performance – turned on



# Evaluation & Future Work

- Implementation done
- The Shuffler – poor performance
- Memory and disk forensics
- The client for the logging module lacks features
- Optimal logging strategy

# Summary

- Implemented a privacy-friendly secure logging module into the PRIME Core
- Investigated the effect of HSQLDB on the privacy properties of our log
- Evaluated our work and found several areas that needs to be further researched

# The Big Picture