IFIP WG10.4 meeting

Report on Session #4

Xavier Défago

School of Computing

Tokyo Institute of Technology

June 2024

S4.1: Yulei Sui's Talk

- **Context**
  - Path-Sensitive Abstract Execution for Software Vulnerability Detection
- **Aim / Highlights**
  - AST —> value-flow paths —> GNN
  - find / predict software vulnerabilities
  - can help/guide classical static analysis
- **Discussions**
  - application to parallel/concurrent programs?
  - …

S4.2: Xingliang Yuan's Talk

- **Context**
  - Securing Graph Neural Networks in MLaaS
- **Aim / Highlights**
  - privacy-preserving ML
  - use function secret sharing
  - Oblivious GNN: prevent leak (training data / model parameters)
  - prevent data misuse; unlearning
- **Discussion highlights**
  - difficulties / needs of unlearning?
  - overhead, …

Some Take-Aways

- **Presentations**
  - both about GNNs
  - GNNs for software dependability *(Yulei)*
  - dependability of ML infrastructure *(Xingliang)*
- **Key points**
  - *(opinionated)*
  - ML/AI techniques not exclusive to classical approaches
  - GNNs for dependability/security
  - dependability/security for GNNs