Research
Publications
Teaching
People
Partners
Resources
News
Jobs
Contact
About NISlab
The Norwegian Biometrics Laboratory
Forensic Laboratory

Process Tracking for Forensic Readiness in OS

Forensic analysis of computer systems suffers from a sparseness of logging of events. It would be desirable to have a log of all state-changing activities of important processes, analogous to a flight data recorder used to investigate plane crashes. Growth in computational power and storage capacity appears to make comprehensive traceability feasible. Traceability provides evidence that can be used in a legal process to achieve accountability of entities. Logging and versioning is a feature increasingly being integrated into platforms and is also mentioned as part of the CRA Grand Research Challenge 4 in Information Systems ("*Build Systems You Can Count On"*).

Challenges that should be addressed by the research include:

- What are the state-changing activities of processes?
- How effective, efficient, and expensive is comprehensive process activity tracking?
- Which hardware/software architecture facilitates process activity tracking?
- What are privacy implications for users of systems that support comprehensive traceability?
- How does comprehensive traceability affect evidence gathering and the legal process?
- How can traceability be generalised to a "unified theory'' of database transactions, configuration changes in system management, and event recovery in forensic investigation?

Methods that can be applied are modelling of operating system and protection mechanisms, architectural analysis of system designs, reasoning about traceable state changes, vulnerability analysis of logging infrastructure, feasibility study of comprehensive traceability by prototypical development.

Specific background and skills in one or more of the following areas is highly desirable:

- Degrees in Computer Science or Engineering with a solid background in operating systems and their APIs, i.e., intimate familiarity with Windows and/or Linux;
- Software development skills;
- Willingness and ability to communicate with people who do not have a technical background.

For more technical information on this positions, please contact Ass.Prof. Hanno Langweg (hanno.langweg@hig.no).

General information on this or other positions at NISlab can be provided by the head of NISlab, Ass.Prof. Patrick Bours (patrick.bours@hig.no). All the above position will soon be officially announced at http://english.hig.no/about/vacancies (or http://www.hig.no/om_hig/ledige_stillinger for the norwegian version).

11/15/2011

PO Box 191, Teknologivn. 22, N-2802 Gjøvik, Phone. (+47) 61135100, Fax (+47) 61135170, E-mail: postmottak@hig.no