Detecting timing attacks using formal methods

PI: Étienne André
Email: phd.promis@lipn13.fr
Laboratory: LORIA, Université de Lorraine, CNRS, Inria, Nancy, France
Team: MOSEL + VeriDis

1 Context

The Spectre vulnerability in modern processors has been reported in 2018. The key insight is that speculative execution in processors can be misused to access secrets speculatively. Subsequently even though the speculatively executed states are squashed, the secret may linger in micro-architectural data structures such as cache, and hence can be potentially accessed by an attacker via side channels.

The Spectre vulnerability is merely one example of a family of vulnerabilities which could lead to the so-called side channel attacks. In general, side channel attacks use information which is leaked through certain side channel (e.g. time, energy (see Fig. 1), cache state and sound wave) in order to reveal system secrets. For instance, a timing side channel attack simply observes variations in how long it takes to perform certain operations, and determines the value of certain secret (e.g. an encryption key) in the system. Such attacks involve analysis of timing measurements and have been demonstrated to be effective in attacking a range of systems.

2 PhD subject

Timing side channel attacks consist in retrieving some secret by taking advantage of some timing information—typically the execution time of a program, or some subfunction. Timing side channel attacks are known to be challenging to detect and mitigate. The goal will be to propose a formal approach so as to verify whether a given system model is free from timing side channel attacks.

Figure 1: An example of power attack (author: Audriusa, license GNU-GPL)
To this end, the system would be modeled using a formalism close to the popular model of
timed automata [AD94], an extension of finite-state automata with real-valued clocks. Then, new
methods should be proposed to detect whether a given system is free from timing side channel
attack or not.

A focus will particularly be made on the case when some of the timing parameters can be con-
figured (e.g. using some `wait` statement in a program). The formalism can then become paramet-
ric timed automata [AHV93], and the ultimate goal will be to synthesize some of these parameter
valuations guaranteeing that the system is free from timing side channel attacks.

The work would contain a theoretical part, but also an implementation part; this implementa-
tion may reuse the parametric timed model checker IMITATOR [And+12].

As a more open research direction, translating real-world programs to parametric timed au-
tomata (or similar formalisms) using only the relevant timing information would also be a possible
research perspective, depending on the applicant’s wish.

**Related works** Opacity or non-interference in timed automata was studied in several works, not-
tably [Bar+02; GMR07; Cas09; Ben+15; AS19]. These works all suffer from some limitations and,
with the exception of [AS19], were not implemented in dedicated software toolkits.

### 3 Framework

#### 3.1 Scientific framework: ANR-NRF ProMiS

This PhD offer is in the framework of the French-Singaporean ANR-NRF project *ProMiS* (Prov-
able Mitigation of Side Channel through Parametric Verification) 2020-2023. This project involves
LORIA (Nancy, France), LS2N (Nantes, France), Singapore Management University and Singapore
University of Technology of Design (Singapore). While the position is based in Nancy, frequent
interactions will be conducted with the other partners of the project; this may include short- or
medium-length visits to Nantes and/or Singapore partners.

#### 3.2 Location: Nancy

The PhD position will take place at LORIA (Laboratoire lorrain de recherche en informatique et ses
applications) at Université de Lorraine, Nancy. LORIA is an internationally recognized research
laboratory comprising over 400 scientists from 48 nationalities.

*Université de Lorraine* is a dynamic university in the beautiful city of Nancy, 1h30 from Paris
by TGV (high-speed train); Nancy is a human-sized city featuring a high quality of life, a UNESCO-
world-heritage city center, and very affordable living costs.
4 Keywords

Formal methods, cybersecurity, verification, opacity, cryptography, program analysis, timed automata

Conditions

Highly motivated applicants with an excellent research record are being sought. Expertise is at least one of the aforementioned keywords is very welcome.

The successful applicant will start on October 1st, 2020.

Approximate remuneration: 1,500 € net / month (social security and retirement scheme are also provided); however, this amount can be increased with a limited amount of teaching. Funding for traveling, notably to Singapore, is also provided.

Application

Applications can be made by email, using a fully developed CV, a research record (if any), Master grades, possible names of referees, and any relevant additional information.

Contact: phd.promis@lipn13.fr
References


