PhD project proposal

Cybersecurity of Real-Time Systems

Supervisors Yann Thierry-Mieg, Dylan Marinho

Laboratory LIP6, CNRS UMR 7606, Sorbonne Université

Team MoVe (Modeling and Verification)

Keywords secure system design · real-time communicating systems · network security · timing attacks · execution-time opacity · parametric timed automata · formal verification

1. General Context

Cyber-attacks that steal confidential information are becoming increasingly frequent and devastating as modern software systems store and manipulate greater amounts of sensitive data. Leaking information about private user data, such as financial and medical records of individuals, trade secrets of companies, or military secrets of states, can have drastic consequences. Although programs that have access to secret information are expected to protect it, many software systems contain vulnerabilities that unintentionally leak information. By observing non-functional side effects such as execution time or memory usage, **side-channel attacks** can capture secret information. Though side-channel vulnerabilities have been known for decades, they are still often neglected by software developers. They are commonly thought of as impractical despite a growing number of demonstrations of realistic side-channel attacks that result in critical security vulnerabilities.

Exploitable timing side channels have been identified in Google's Keyczar Library[1] and in multiple implementations of RSA [BB05] and elliptic-curve cryptography [BT11]. An external attacker or malicious observer can infer sensitive information (secret keys, private states, or confidential behaviors) simply by measuring observable response delays or execution times over the network. In the context of communication and networks, such timing leaks represent a critical threat to the confidentiality of data exchanges and the overall resilience of the system.

A defining real-world example is the series of remote timing attacks against OpenSSL. In their seminal work [BB05], Brumley and Boneh demonstrated that an attacker could recover a 1024-bit RSA private key from an OpenSSL server by measuring network response times, using approximately one million queries over about two hours. Eight years later, in [BT11], Brumley and Tuveri showed that remote timing attacks remained practical against OpenSSL's elliptic-curve implementations, despite intervening countermeasures. These attacks highlight how subtle timing variations dependent on secret data can be exploited remotely. Despite the countermeasures implemented since then, timing

[1] https://rdist.root.org/2009/05/28/timing-attack-in-google-keyczar-library/

side-channel attacks continue to be regularly demonstrated on modern protocols. For instance, several QUIC[2] implementations remain vulnerable to timing leaks arising from non-constant-time processing of data at secret offsets [Dou22], while comprehensive surveys highlight persistent timing-related privacy and security issues in QUIC deployments [JF24].

To counter such threats, we study a fundamental security property called **opacity**. Opacity ensures that an external observer cannot distinguish, based in particular on execution times and communication delays, whether the system is executing a secret behavior or an equivalent public behavior. The methods developed in this PhD—parametric modeling, execution-time opacity verification, and synthesis of parameters or controllers—would enable the detection of these leaks at design time and the automatic enforcement of strong timing-based security guarantees.

2. Scientific Context

We consider parametric real-time communicating systems that allow to represent both the timing constraints of the network and the uncertainties or design freedoms of the system (via parameters). We will use **parametric timed automata (PTAs)** [AHV93], a natural extension of timed automata (TAs). Building on previous work introducing **execution-time opacity** (ET-opacity) [ALM+22] [ALL+23], we are interested in verifying properties of C programs by studying their timing aspects. For this purpose, an automatic translation of C programs to formal timed models was prototyped [ABC+25], enabling the verification of ET-opacity properties on real code. This PhD project will extend this line of research by improving the translation toolchain for greater scalability and realism, while developing new techniques for parameter synthesis and timed control to enforce opacity properties.

3. Objectives

This PhD will study the verification and synthesis of timed opacity properties in real-time communicating systems and networks, along two complementary research directions.

- **Parametric systems**: Synthesis of parameter values that ensure a real-time communicating system (*e.g.* a protocol or controller) satisfies opacity, despite uncertainties on transmission delays or hardware performance. This provides strong design-time guarantees during the modeling phase of the system.
- **Controllable systems**: Introduction of control mechanisms (supervisors or security controllers) that dynamically restrict the system's behaviors in order to preserve opacity against possible attacker actions on the network.

Thus, the PhD will contribute to the **design** of real-time communicating systems that are **robust** against timing-based attacks and provide **formal guarantees** of security properties. We expect the development of prototypes and open-source tools in addition to theoretical results, in order to demonstrate the applicability of the developed methods. These directions combine a strong theoretical component (formal verification, parameter synthesis, controller synthesis) with concrete

[2] a modern transport protocol aiming to improve web connection performance and security

applications in the cybersecurity of communicating systems (*e.g.* secure communication protocols, real-time networks, connected embedded systems) in the general context of critical real-time systems. Beyond theoretical contributions, case studies on industrial protocols (*e.g.* real-time control-command protocols) will be conducted to validate the relevance of the proposed techniques.

References

[AHV93] Rajeev Alur, Thomas A. Henzinger, and Moshe Y. Vardi. "Parametric real-time reasoning". In: *STOC*. Edited by S. Rao Kosaraju, David S. Johnson, and Alok Aggarwal. San Diego, California, United States: ACM, 1993. pages 592–601. DOI: 10.1145/167088.167242.

[ABC+25] Étienne André, Jean-Luc Béchennec, Sudipta Chattopadhyay, Sébastien Faucou, Didier Lime, **Dylan Marinho**, Olivier H. Roux, and Jun Sun. "Verifying Timed Properties of Programs in IoT nodes using Parametric Time Petri Nets". In: *SAC 2025*. Edited by Jiman Hong, Sebastiano Battiato, Christian Esposito, Juw Won Park, and Adam Przybylek. Catania, Italy: ACM, 2025. pages 1998–2006. DOI: 10.1145/3672608.3707861.

[ALL+23] Étienne André, Engel Lefaucheux, Didier Lime, **Dylan Marinho**, and Sun Jun. "Configuring Timing Parameters to Ensure Execution-Time Opacity in Timed Automata". In: *TiCSA@ETAPS 2023*. Edited by Maurice H. Beek and Clemens Dubslaff. EPTCS. Paris, France, 2023. pages 1–26. DOI: 10.4204/EPTCS.392.1.

[ALM+22] Étienne André, Didier Lime, **Dylan Marinho**, and Sun Jun. "Guaranteeing timed opacity using parametric timed model checking". In: *ACM Transactions on Software Engineering and Methodology* 31.4 (2022), pages 64:1–64:36. DOI: 10.1145/3502851.

[BT11] Billy Bob Brumley and Nicola Tuveri. "Remote Timing Attacks Are Still Practical". In: *ESORICS 2011*. Edited by Vijay Atluri and Claudia Díaz. Lecture Notes in Computer Science. Leuven, Belgium: Springer, 2011. pages 355–371. DOI: 10.1007/978-3-642-23822-2_20.

[BB05] David Brumley and Dan Boneh. "Remote timing attacks are practical". In: *Computer Networks* 48.5 (2005), pages 701–716. DOI: 10.1016/J.COMNET.2005.01.010.

[Dou22] Gérald Doussot. *Constant-Time Data Processing At a Secret Offset, Privacy and QUIC*. Edited by NCC Group Research. 5 September 2022. URL: https://www.nccgroup.com/research/constant-time-data-processing-at-a-secret-offset-privacy-and-quic/.

[JF24] Y A Joarder and Carol J. Fung. "Exploring QUIC Security and Privacy: A Comprehensive Survey on QUIC Security and Privacy Vulnerabilities, Threats, Attacks, and Future Research Directions". In: *IEEE Transactions on Network and Service Management* 21.6 (2024), pages 6953–6973. DOI: 10.1109/TNSM.2024.3457858.