POLITECNICO DI TORINO

Dipartimento di Automatica e Informatica

PhD in Computer and Control Engineering

XXXII cycle

Supervisor

*Prof. Gianpiero Cabodi*

# Cybersecurity for embedded systems: methodologies, techniques and tools

PhD Candidate: *SEBASTIANO FABRIZIO FINOCCHIARO*

## 1. Introduction / Context

Our society, economy, and critical infrastructures have become largely dependent on computer networks and embedded systems. New security attacks, like Spectre and Meltdown, have a groundbreaking impact on our society because they underline vulnerabilities in hardware designs that have been going unnoticed for years. This shows the weakness of the state-of-the-art verification process and design practices.

## 2. Goal / Objectives

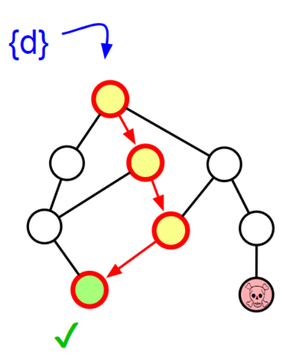
The goal of this PhD thesis is to extend state-of-the-art verification methodologies for cybersecurity and offer new approaches in embedded systems.

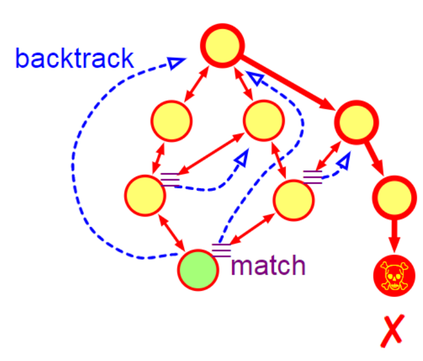
## 3. Method

This PhD work can be divided in two tracks: formal and non-formal verification methods.

As regards to the latter, efforts were given to static, dynamic and mixed code testing techniques (e.g. symbolic execution, dynamic taint analysis, etc.).

Though they require little manual effort and they tend to be more automatic, compared to other methods, these techniques are far from being complete, i.e. they do not explore the whole state space.



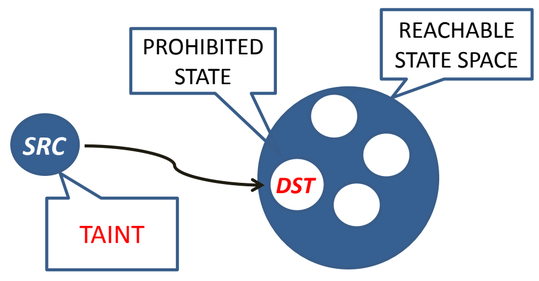



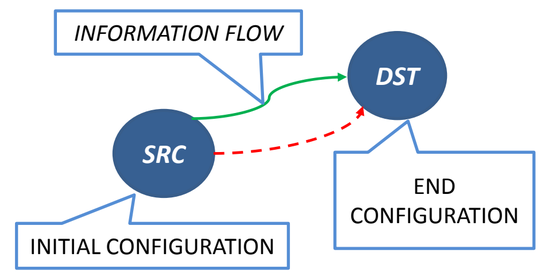

Conversely, formal methods, for example model checking or equivalence checking, are proven to be complete but they lack of automation and usually require a lot of human effort.

A first key contribution in this field is the definition of new security-related properties.

State Property (SP) is a class of properties that captures state-related behaviours, e.g. unwanted or illegal states.

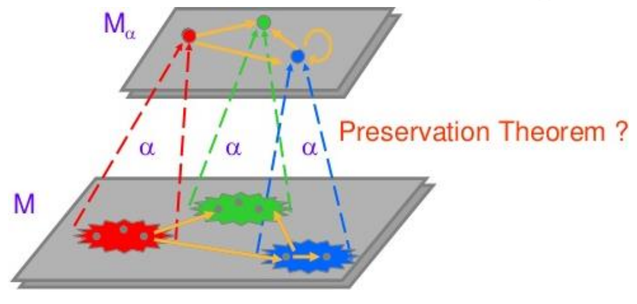
Path Property (PP), instead, deals with information flow-related behaviours, e.g. unwanted or illegal paths.




Another key contribution in this track is a novel verification approach based on taint analysis for speculative attacks, e.g. Spectre and Meltdown.

A processor model is usually too big to be verified with a standard model checker, therefore this work presents an abstraction and reduction-based approach alongside with taint propagation to verify security flaws in OOO processor designs.




## 4. Results

Portfolios of State and Path properties have been defined. A verification approach to verify them has also been presented. Another approach in verifying security properties in pipelined out-of-order processors that can be applied to check speculation-based vulnerabilities has also been introduced. Experiments have been conducted on real architectures and experimental results support the feasibility of the claims.

## 5. References

1. Cabodi, G. et al. (2016) “Secure Path Verification”. In: IEEE International Verification and Security Workshop.
2. Cabodi, G. et al. (2017) "Embedded systems secure path verification at the hardware/ software interface." IEEE Design & Test 34.5: 38-46.
3. Cabodi, G. et al. (2019) “Model Checking Speculation-Dependent Security Properties: Abstracting and Reducing Processor Models for Sound and Complete Verification”. In: Electronics 2019, 8, 1057- ISSN 2079-9292.