For Women in Science

UNESCO | FONDATION L'ORÉAL

AUTOMATED PROGRAM ANALYSIS FROM SAFETY TO HYPERSAFETY

Thursday, 8th October, 2020

PROGRAMS MANIPULATE SECRET DATA

- **Critical software are prevalent**

  → Secure internet communications

  → Secure banking transactions

  → Manipulate health data

- **Rely on cryptography**

  → Cryptography offers **mathematical guarantees**

  → **Verified** implementations (no bugs, functional)

  → *But what about execution in the* ***physical world****?*

https
CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

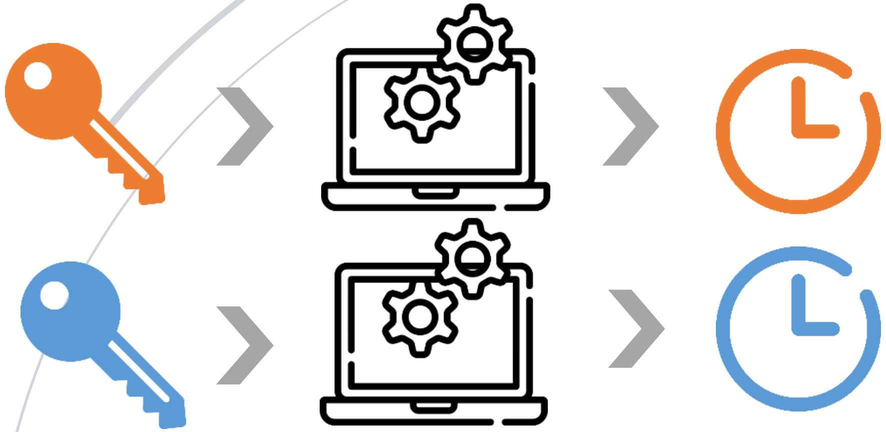
PROTECT SECRETS MANIPULATED BY PROGRAMS
THE CASE OF TIMING ATTACKS

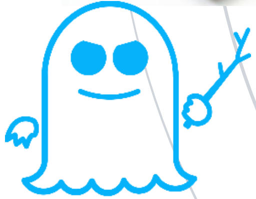
- First timing attack in **1996** by Paul Kocher: full recovery of **RSA encryption key**
- **Timing attacks:** execution time of programs can leak secret information
- **Execution is not easy to determine**

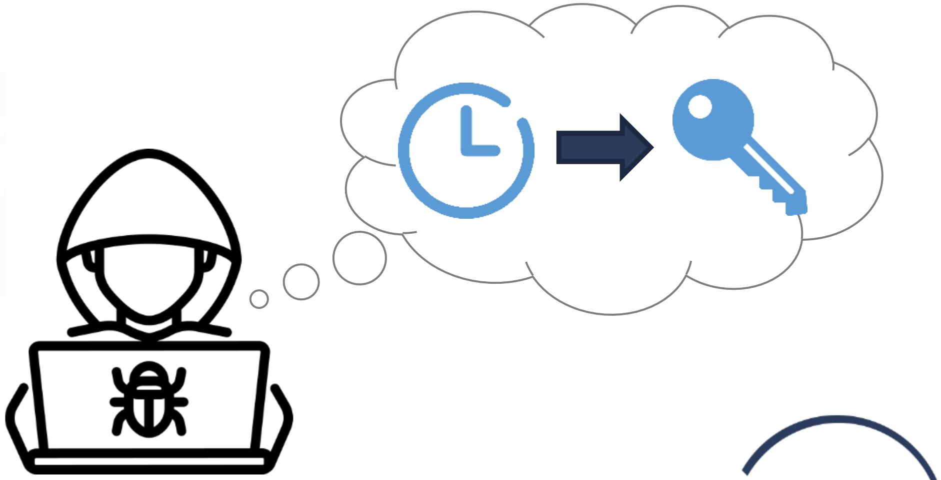
  → Sequence of instructions executed

  → Memory accesses (Cache attacks, 2005)

  → Speculation (Spectre attacks, 2018)





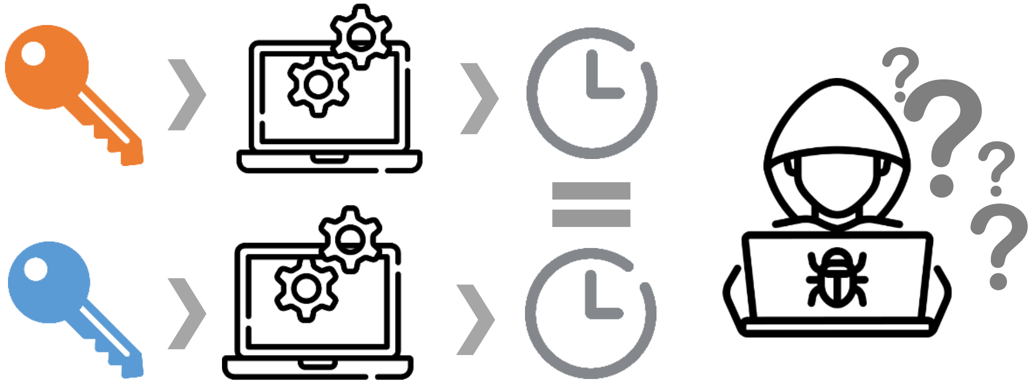


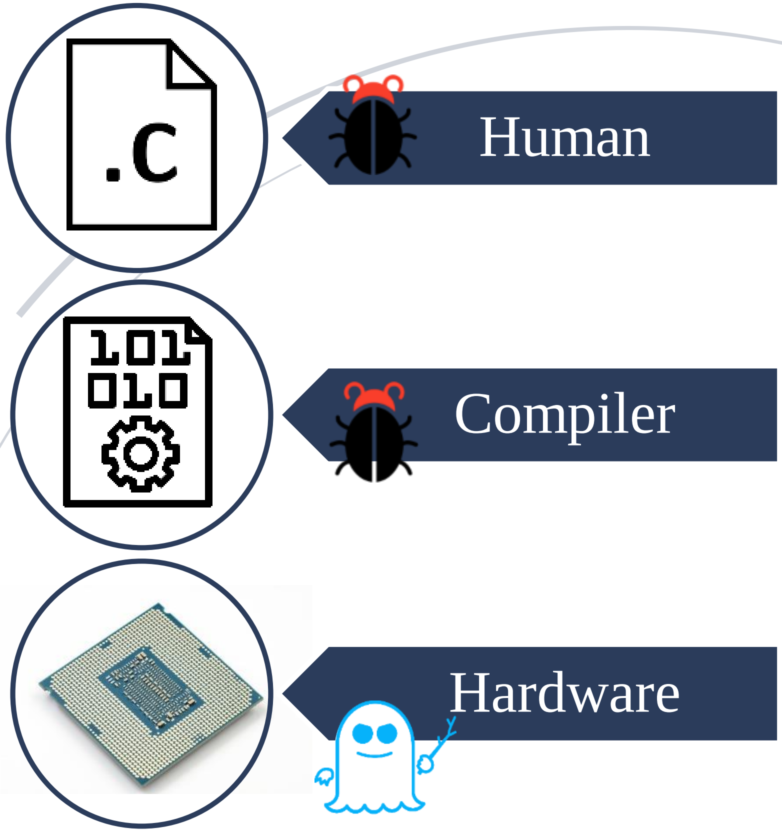
CONSTANT-TIME PROGRAMMING

A SOLUTION AGAINST TIMING ATTACKS

- Constant-time **programming**

  → Execution time of a program must be independent from secret data





- **Hard to guarantee constant-time**

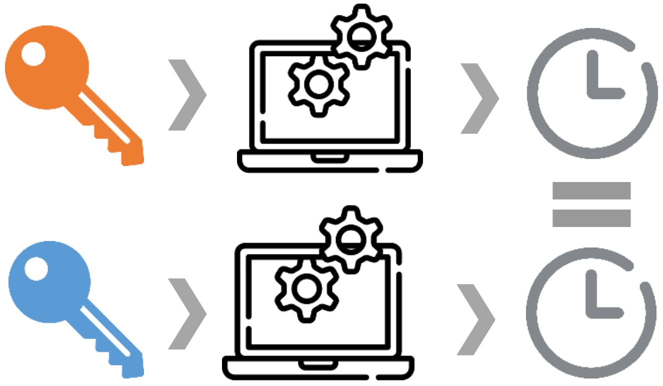
  → Need **automated verification tools**

AUTOMATIC VERIFICATION OF CONSTANT-TIME

THREE CHALLENGES

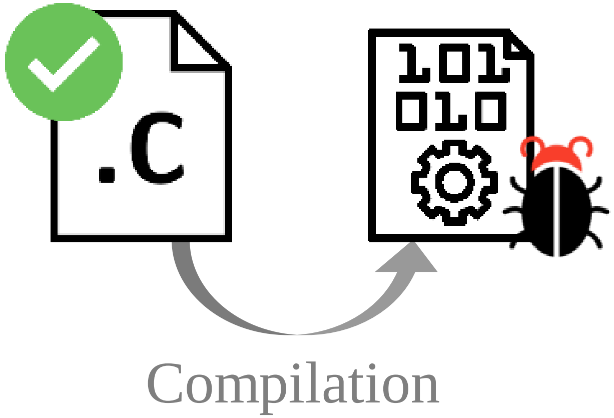
1

Not regular safety but security (**2-hypersafety)**
→ Efficiently model *pairs* of executions



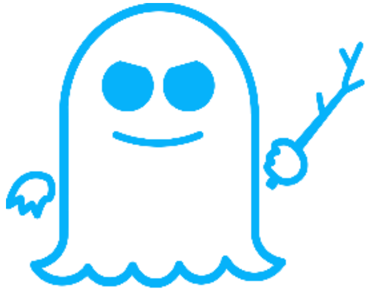
2

Not necessarily preserved by compilers
→ Binary analysis



3

Model efficiently program behavior with **speculative execution**

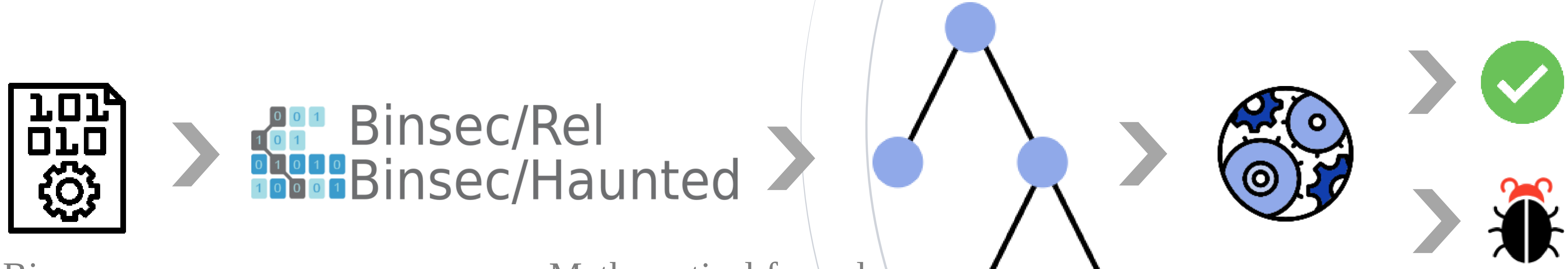


CONTRIBUTION
EFFICIENT AUTOMATED ANALYSIS OF CONSTANT-TIME AT BINARY LEVEL

New Tools:
Binsec/Rel &
Binsec/Haunted

Efficient: based on
dedicated optimizations
(× 700 speedup)

Binsec/Rel effective
on real crypto codes
2 new bugs & 296 proofs



Binary
program

Mathematical formula
of the program

Constraint-solver:
resolves formula

CONCLUSION

- **My Research**

  Efficient automated analysis for security **(2-hypersafety)** at **binary level**

- **Application**

  Constant-time cryptography under **speculative execution**

- **Future Work**

  → Extend Binsec/Rel to **more security properties**
  → Explore **architectural guarantees** for security

Binsec/Rel
Binsec/Haunted