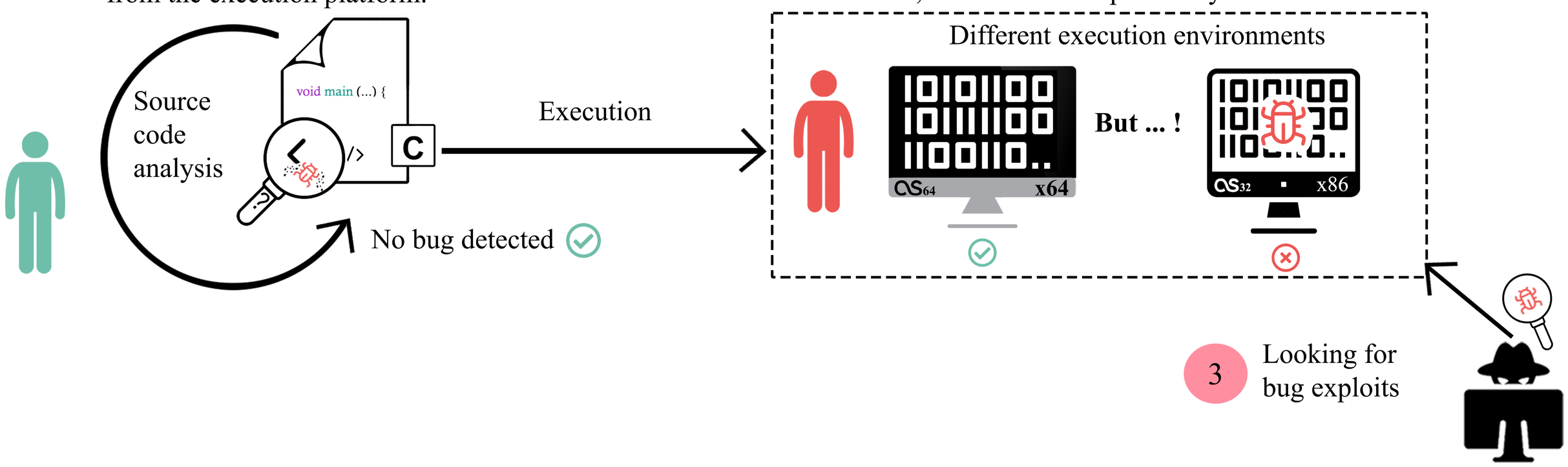
Detection of security vulnerabilities induced by integer errors

Before

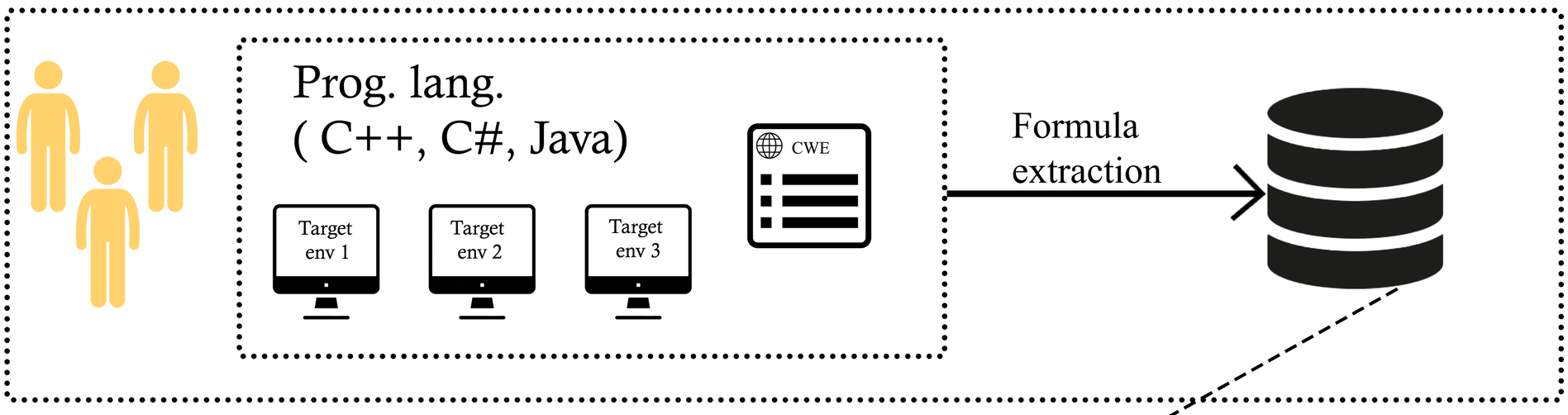
1 Verification concentrates on the correctness of the programs focusing on the source code, independently from the execution platform.

2 Depending on the platform used for the execution, some flaws in computer software causes an unintended behavior to occur on safe code, which can be exploited by a threat actor.



Now

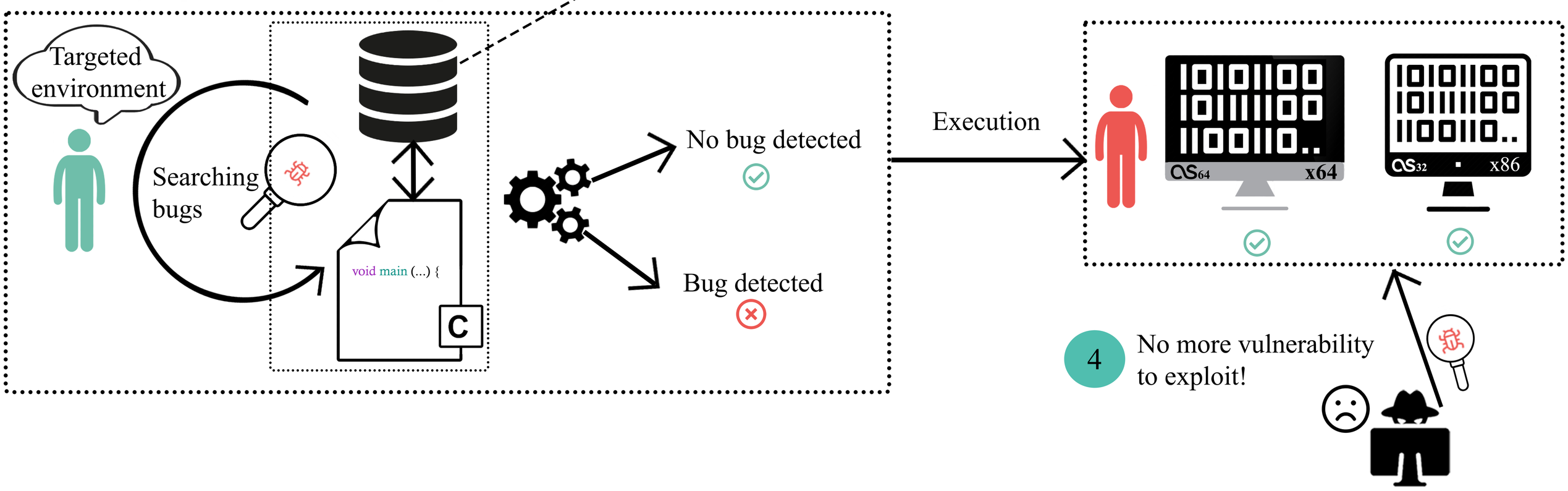
1 Creation of knowledge base by extracting specifications from computing platforms (storage device, compilers, operating systems), Common Weakness Enumeration and programming best practices.



The knowledge base will be avaible for the community.

2 We offer the possibility to automatically discover vulnerabilities. Based on a precise knowledge of the execution context of the analysed program, bug analysis should detect security exploits which it can be repaired.

3 Once the bugs are fixed by developers, the attacker will no longer be able to exploit security vulnerabilities.



Salim Yahia Kissi[1], Yassamine Seladji[1], Rabea Ameur-Boulifa[2]

[1] *LRIT, University of Abou Bekr Belkaid, Tlemcen, Algeria*

[2] *LTCI, Télécom Paris, Institut Polytechnique de Paris, France*

{salimyahia.kissi, yassamine.seladji}@univ-tlemcen.dz

Rabea.Ameur-Boulifa@telecom-paris.fr

جامعة أبو بكر بلقايد

UNIVERSITY OF TLEMCEN

TELECOM Paris

IP PARIS