EPOCHE & ESPRI

The public domain and the CEM attack potential mismatch

10th ICCC Norway

José Francisco Ruiz Gualda

Agenda

- CEM Attack Potential
- Public Domain => Source of Knowledge
- Attack Potential Calculation
  - Issues
  - Problems
- Conclusions

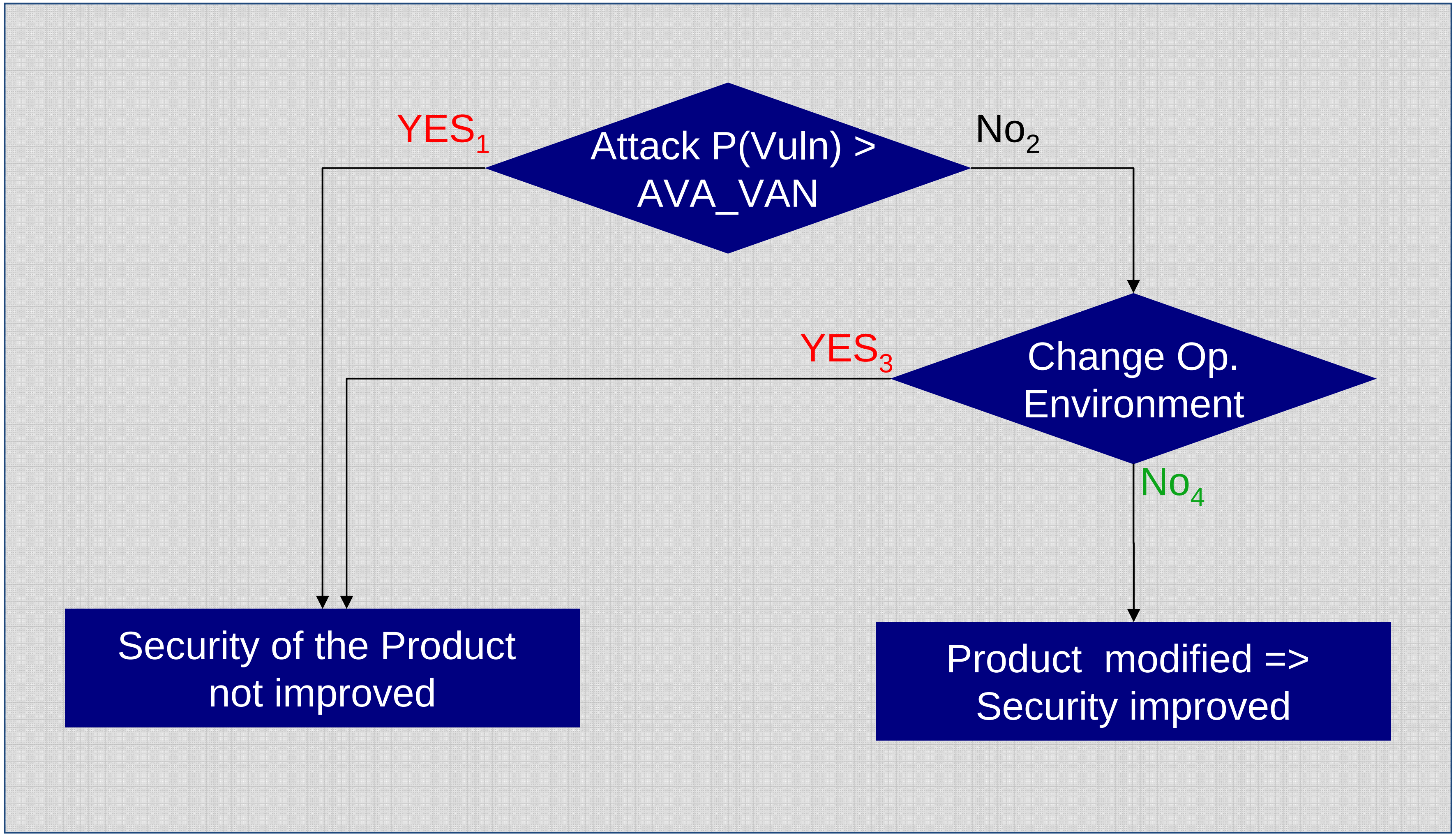
CEM Attack Potential

- Attack Potential
- Factors to be considered:
  - Elapsed time
  - Expertise
  - Knowledge of the TOE
  - Window of Opportunity
  - Equipment

CEM Attack Potential

- Developers
  - Attack potential possessed by the assumed attackers of the TOE.
  - The resistance of the TOE (assurance level).
- Evaluators
  - TOE resistance to attacks assuming a specific attack potential of an attacker.

CEM Attack Potential (Importance)

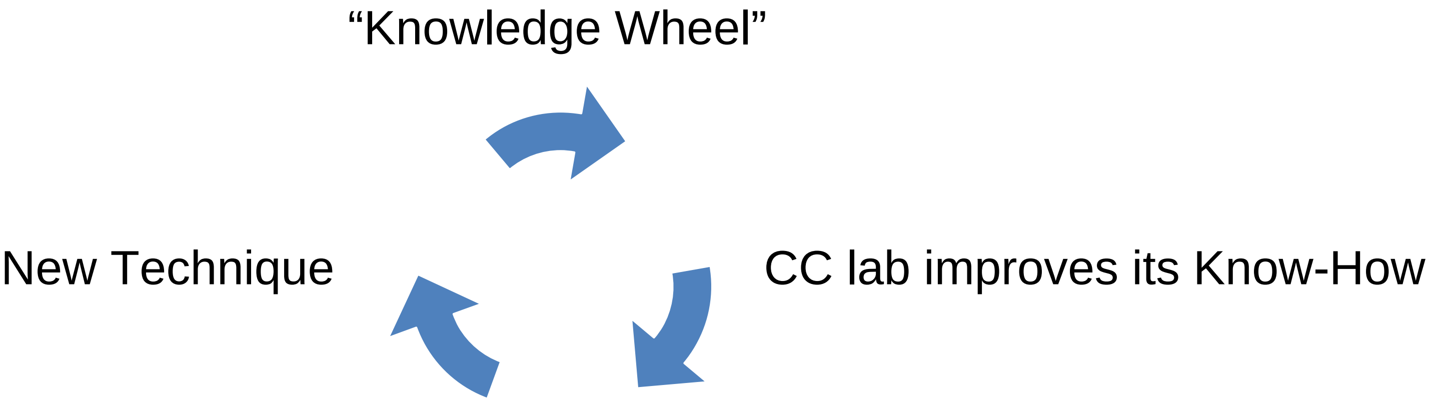

YES1
Attack P(Vuln) > AVA_VAN
No2
YES3
Change Op. Environment
No4
Security of the Product not improved
Product modified => Security improved

Public Domain => Source of Knowledge

- Vulnerabilities
  - Vulnerabilities Databases (CVE Mitre)
  - Vulnerabilities Scanners
- Know-How
  - Own Research
  - New Methods, Techniques…

Public Domain => Source of Knowledge

- Know-How:



“Knowledge Wheel”

CC lab improves its Know-How

New Technique

Public Domain => Source of Knowledge

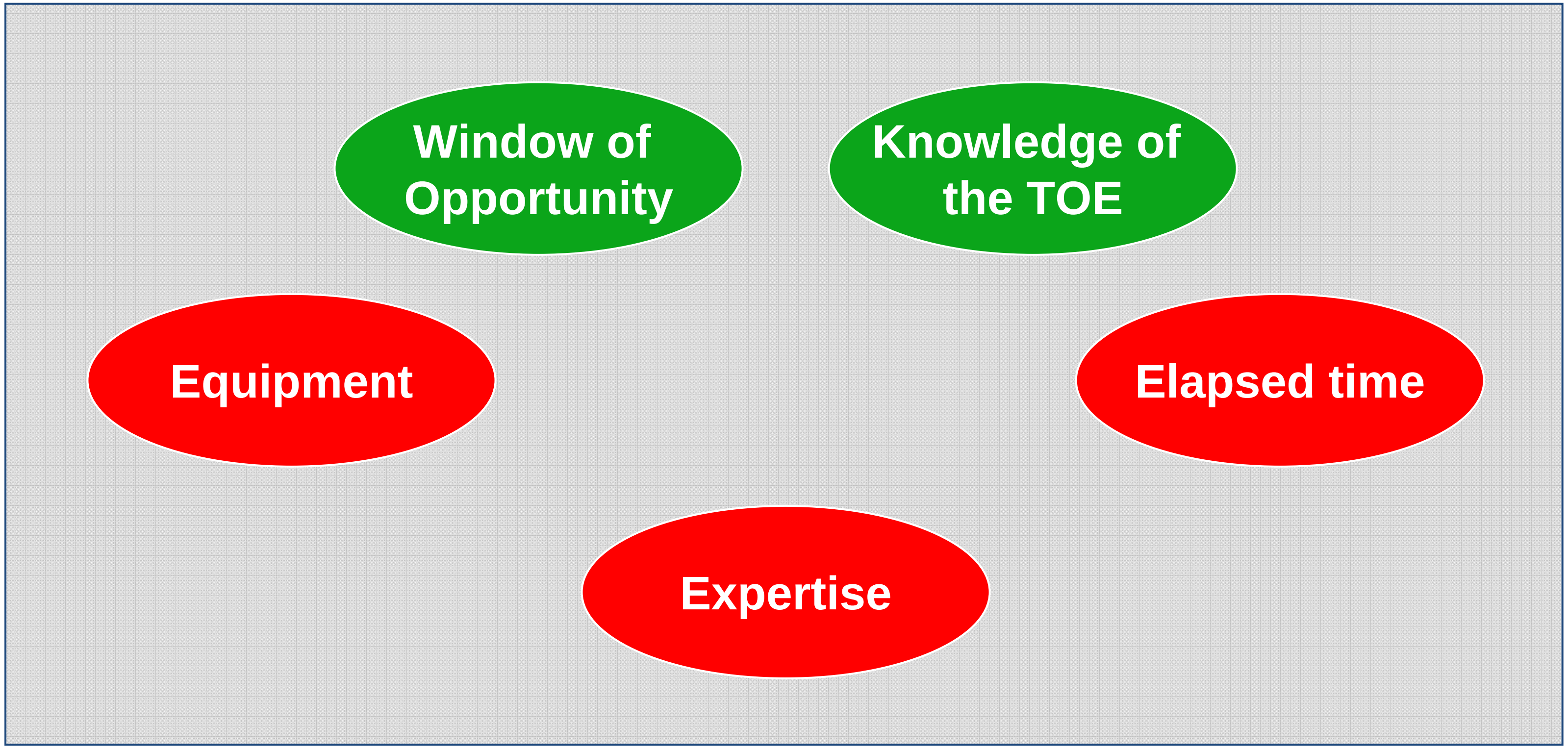
- Example: Exploiting Buffer Overflow
  - Linux
  - Linux with Randomization (ASLR)
  - Linux with Canary values

Attack Potential Calculation

- CC World
  - Motivation: Fun & Money
  - Resources: **Unfortunately limited**
  - Expertise: depending on the technology and the lab
- Real World
  - Motivation: Fun & Money
  - Resources: **Unlimited**
  - Expertise: Experts

Attack Potential Calculation Issues

- CC World vs Real World


Window of Opportunity

Knowledge of the TOE

Equipment

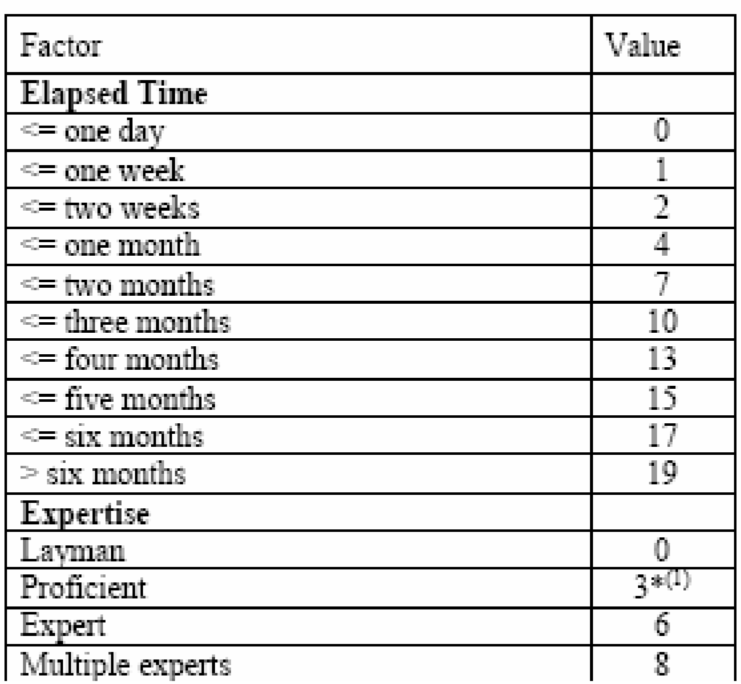
Elapsed time

Expertise

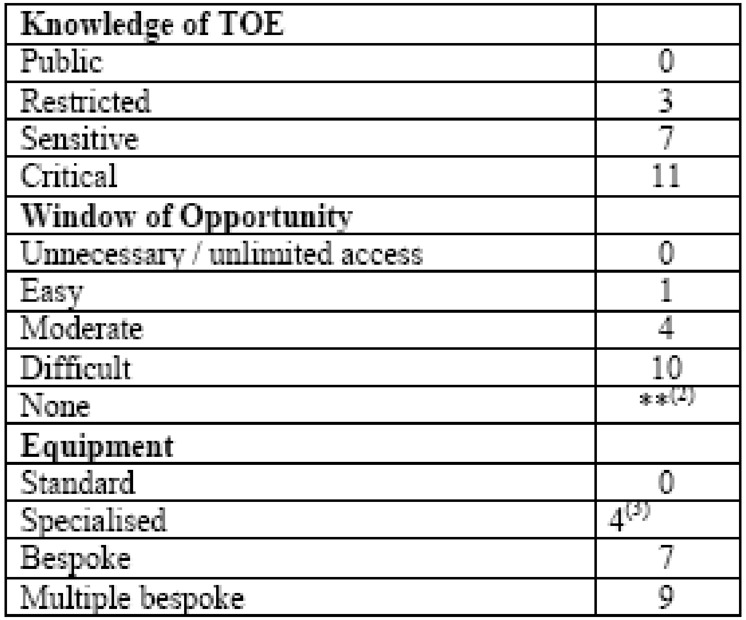
Attack Potential Calculation Issues

- Is any technique inapplicable depending on the assurance level?
  - Rootkits
  - Reverse Engineering
  - …

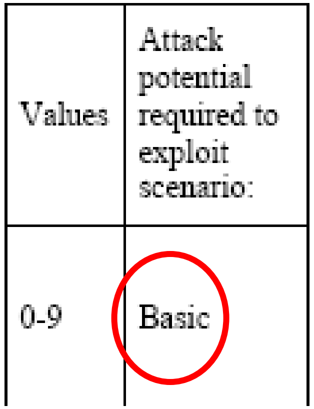
Attack Potential Calculation Issues



Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*(1)
Expert	6
Multiple experts	8



Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**(2)
Equipment	
Standard	0
Specialised	4(3)
Bespoke	7
Multiple bespoke	9



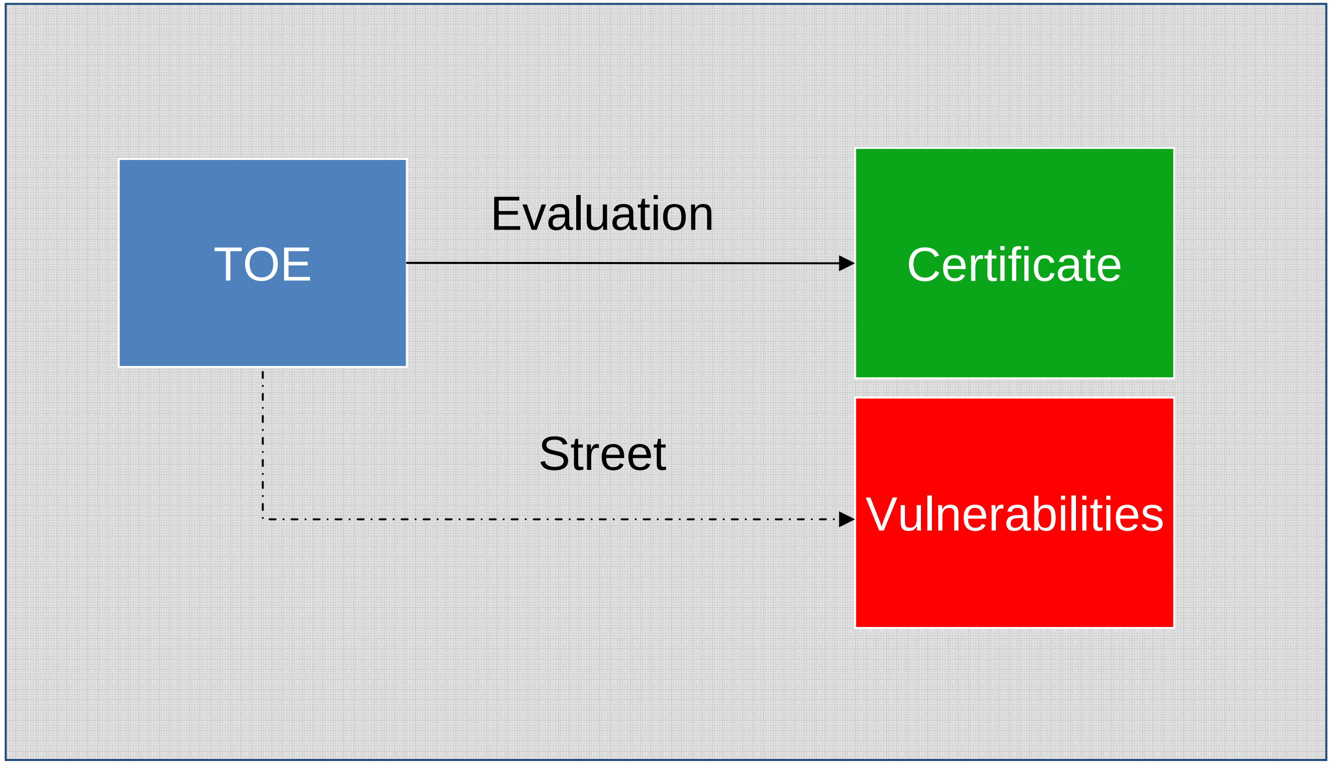
Values	Attack potential required to exploit scenario:
0-9	Basic

Attack Potential Calculation Issues

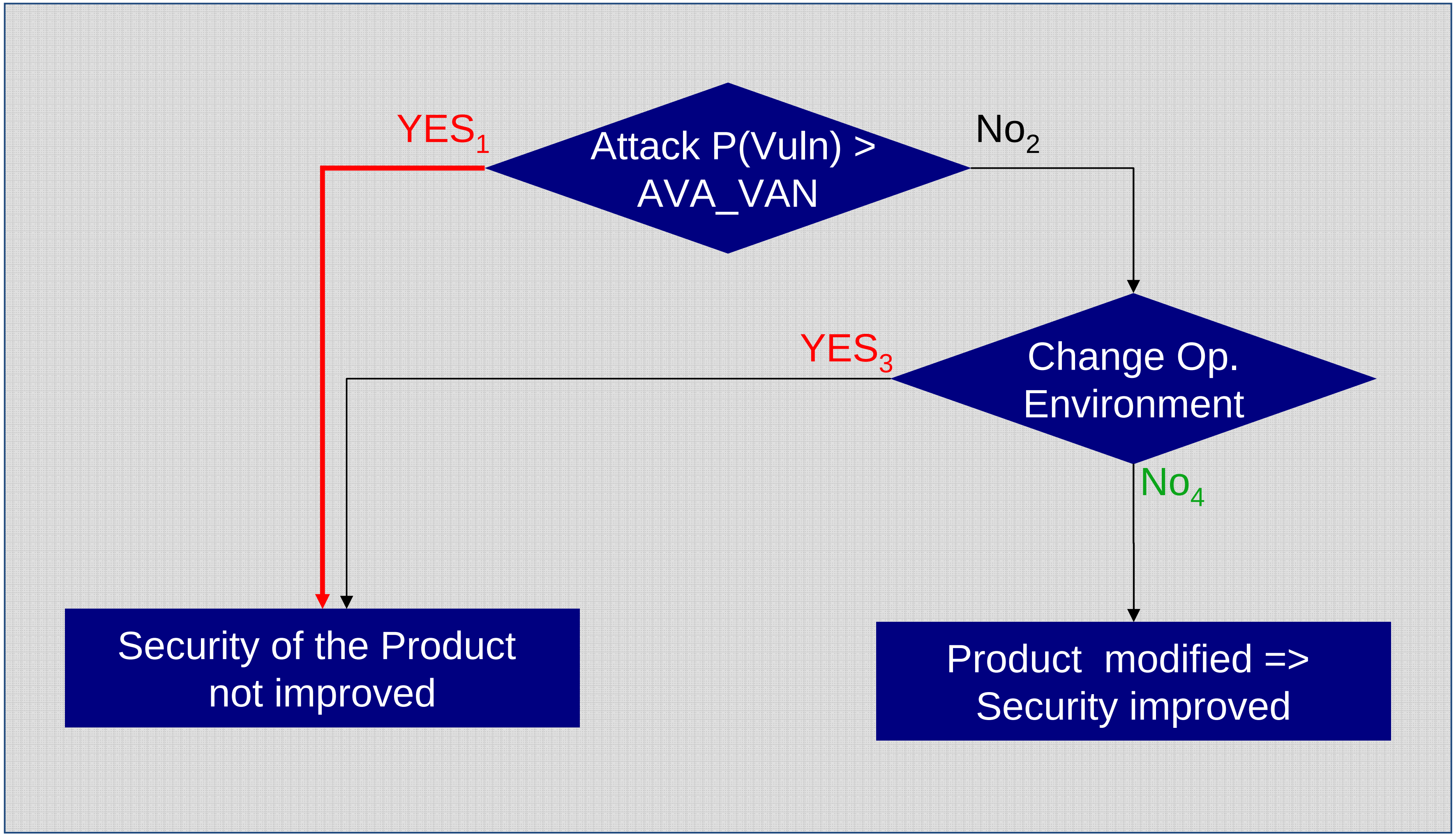
- Is any knowledge inapplicable depending on the assurance level?
  - CEM, paragraph 1915: *“This knowledge is not expected to extend to specific conference proceedings or detailed theses produced by university research for AVA_VAN.1 or AVA_VAN.2.”*

Attack Potential Calculation Problems

- The real world is two steps in front of the CC World



Attack Potential Calculation Problems


YES$_1$
Attack P(Vuln) > AVA_VAN
No$_2$
YES$_3$
Change Op. Environment
No$_4$
Security of the Product not improved
Product modified => Security improved

Attack Potential Calculation Problems

- When a TOE is used in **Restricted** Environments
  - Window of Opportunity and Knowledge of the TOE acquire more importance => A CC Lab shall obtain better results.

Attack Potential Calculation Problems

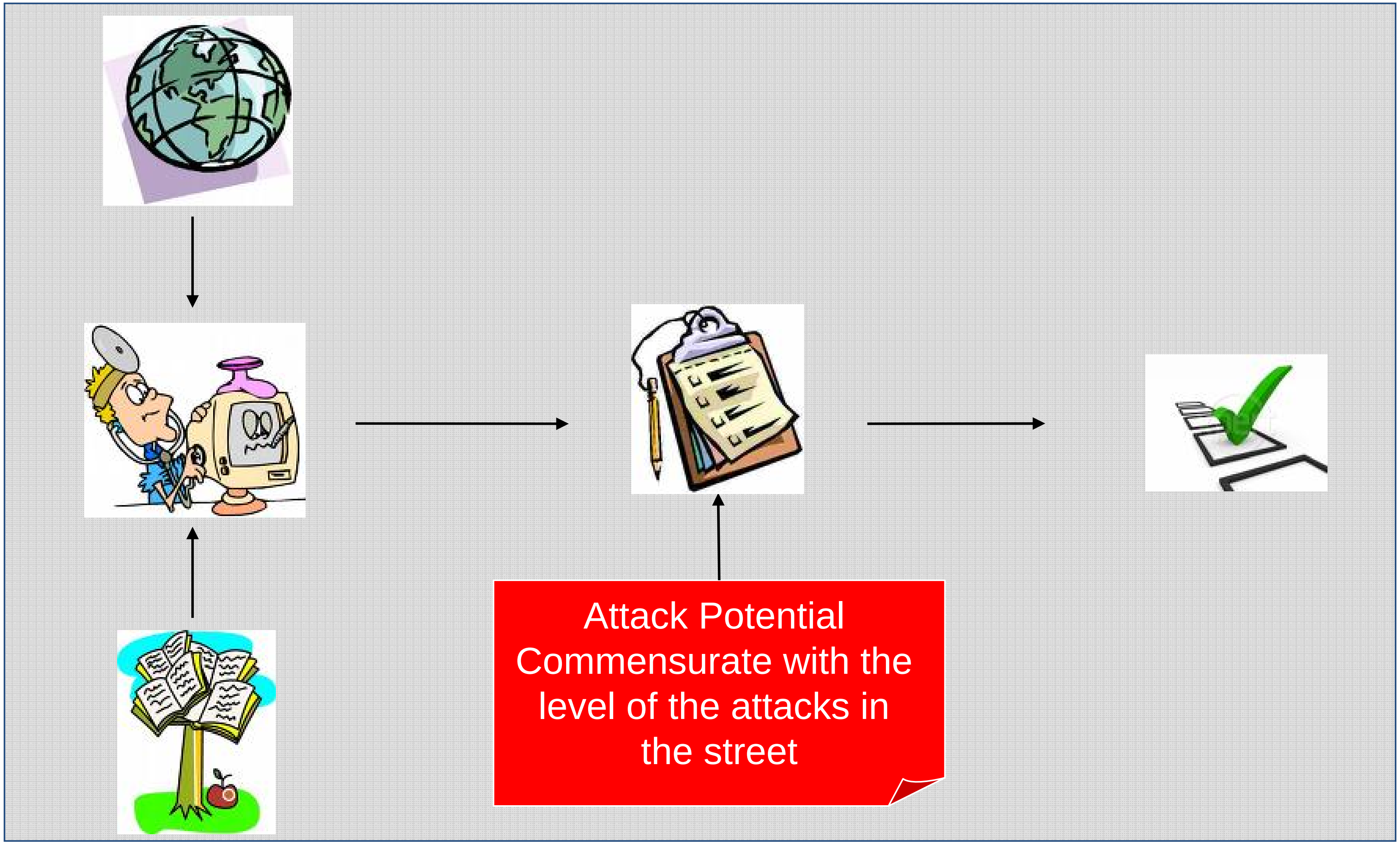
- When a TOE is used in **Public** Environments
  - Attackers have free access to the TOE and knowledge of the TOE => It is difficult to compete with the real world for a CC lab

Conclusions

- The knowledge of CC evaluators shall be up to date with the public domain.

- The Attack Potential Calculation in CC shall be commensurate with the attacks in the street.

Conclusions



Attack Potential Commensurate with the level of the attacks in the street

Questions

Thanks for all!!

?

José Francisco Ruiz Gualda

eval@epoche.es