Exploit Mitigations Outro

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Content

Slides based on excellent presentation:

“Modern Exploit Mitigations”, Swiss CyberStorm 2017

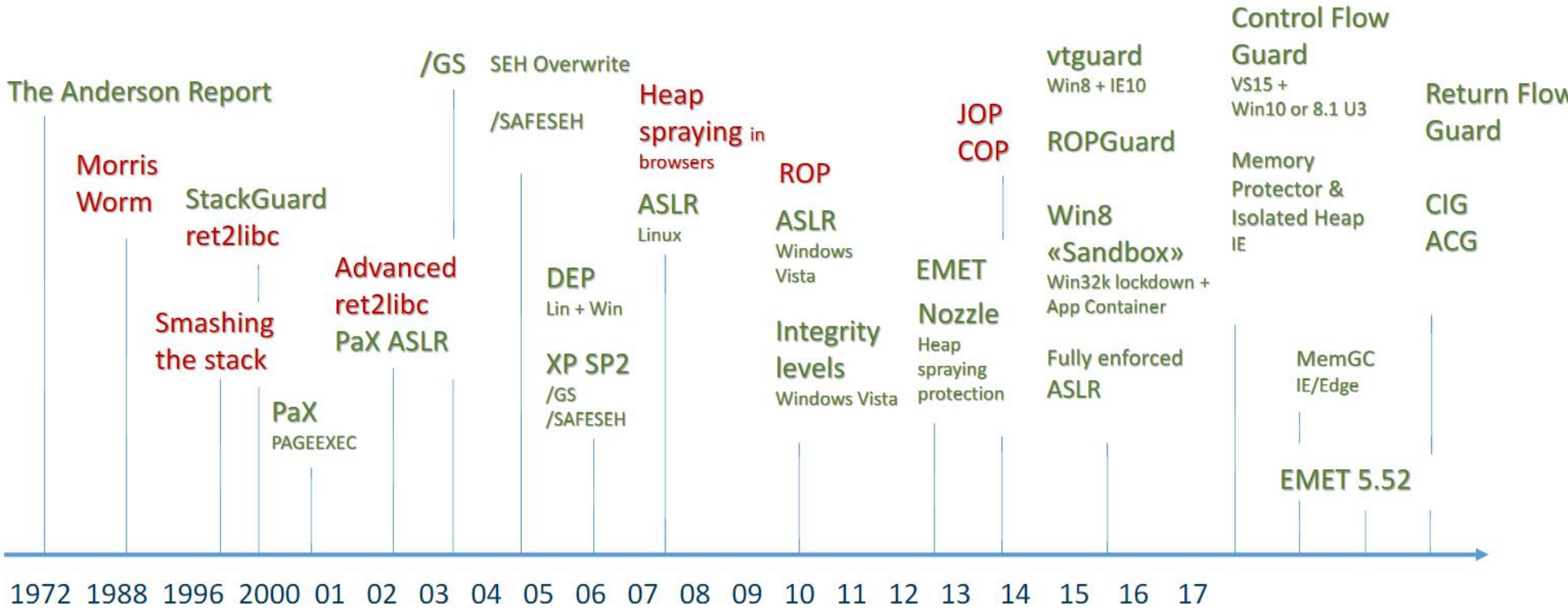
“Compilers, Memory Errors and Hardening Techniques”

- https://www.ethz.ch/content/dam/ethz/special-interest/infk/inst-cs/lst-dam/documents/Education/Classes/Spring2016/2810_Advanced_Compiler_Design/Slides/20160518_advanced_compiler_design.pdf

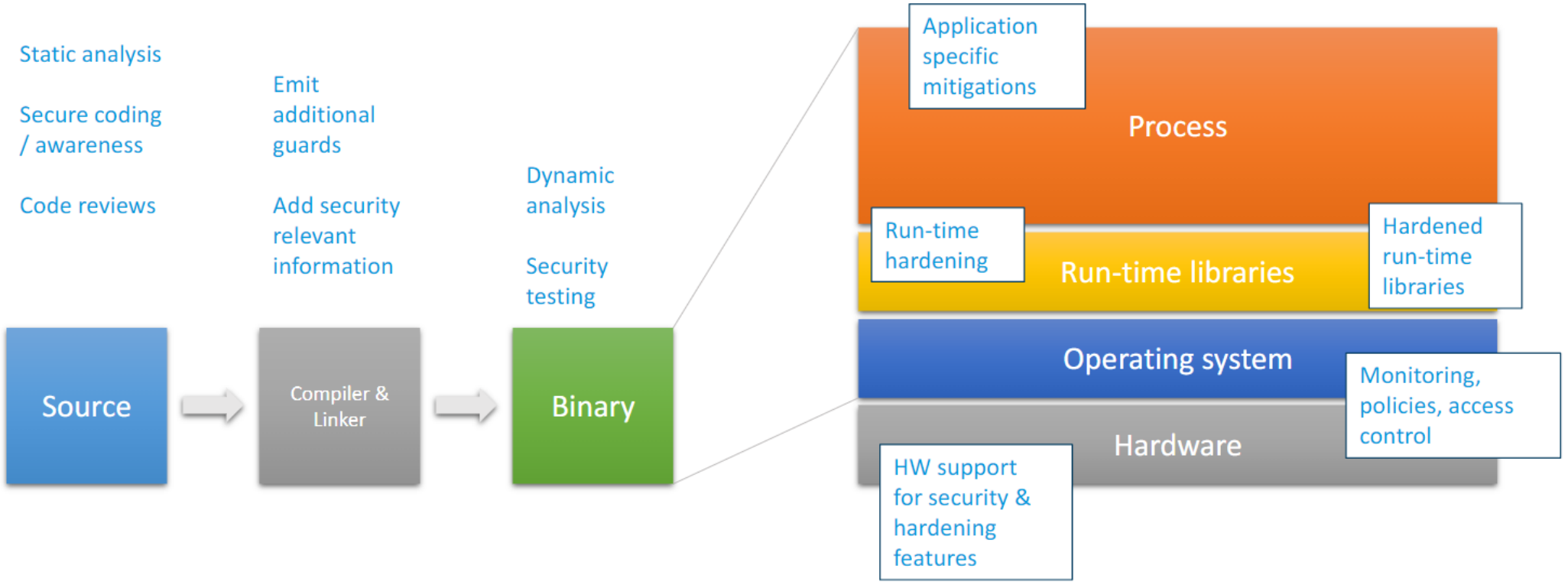
Both by:

- xorlab (ETH Spinoff),
- Matthias Ganz & Antonio Berresi

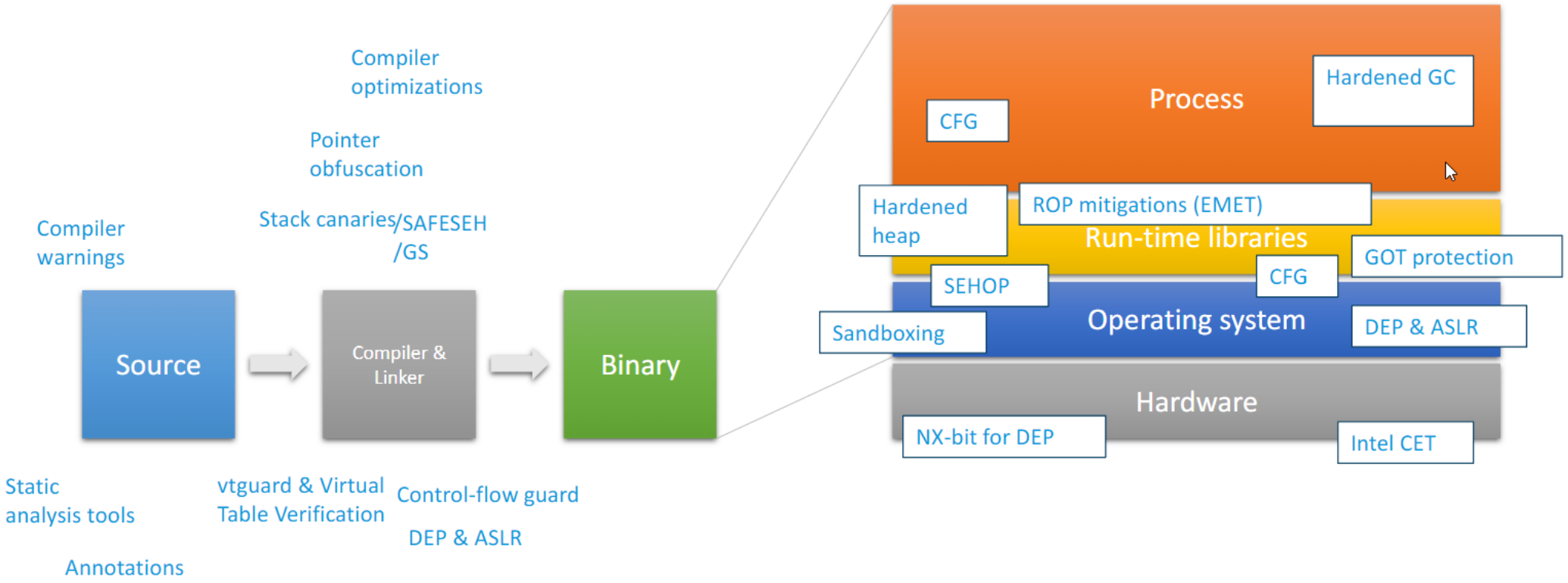
Exploit mitigations since the 90s



Hardening value chain

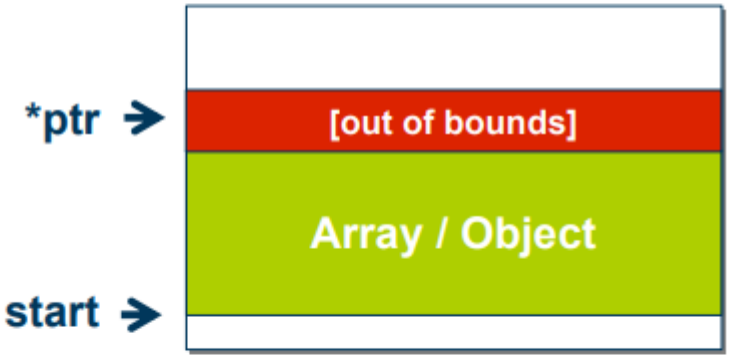


Hardening value chain



Types of memory errors

Spatial error



- De-reference pointer that is out of bounds

Temporal error

- De-reference pointer to freed memory

Types of bugs

- Out-of-bounds bugs / Buffer overflows
  - On stack or heap
- Dangling pointer / Use-after-free
- Integer bugs, signedness bugs
- Format string bugs
- Uninitialized memory
- NULL pointer dereference

Attack types

- Code corruption attack
- **Control-flow hijack attack**
- Data-only attack
- Information leak