



华中科技大学

HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

网络空间安全学院



内存安全漏洞/内存错误漏洞

SoK: Eternal War

László Szekeres[†], Mathias Payer[†]
[†] Stony Brook
[‡] University of California
^{*} Peking University

[SoK: Eternal War in Memory](#)



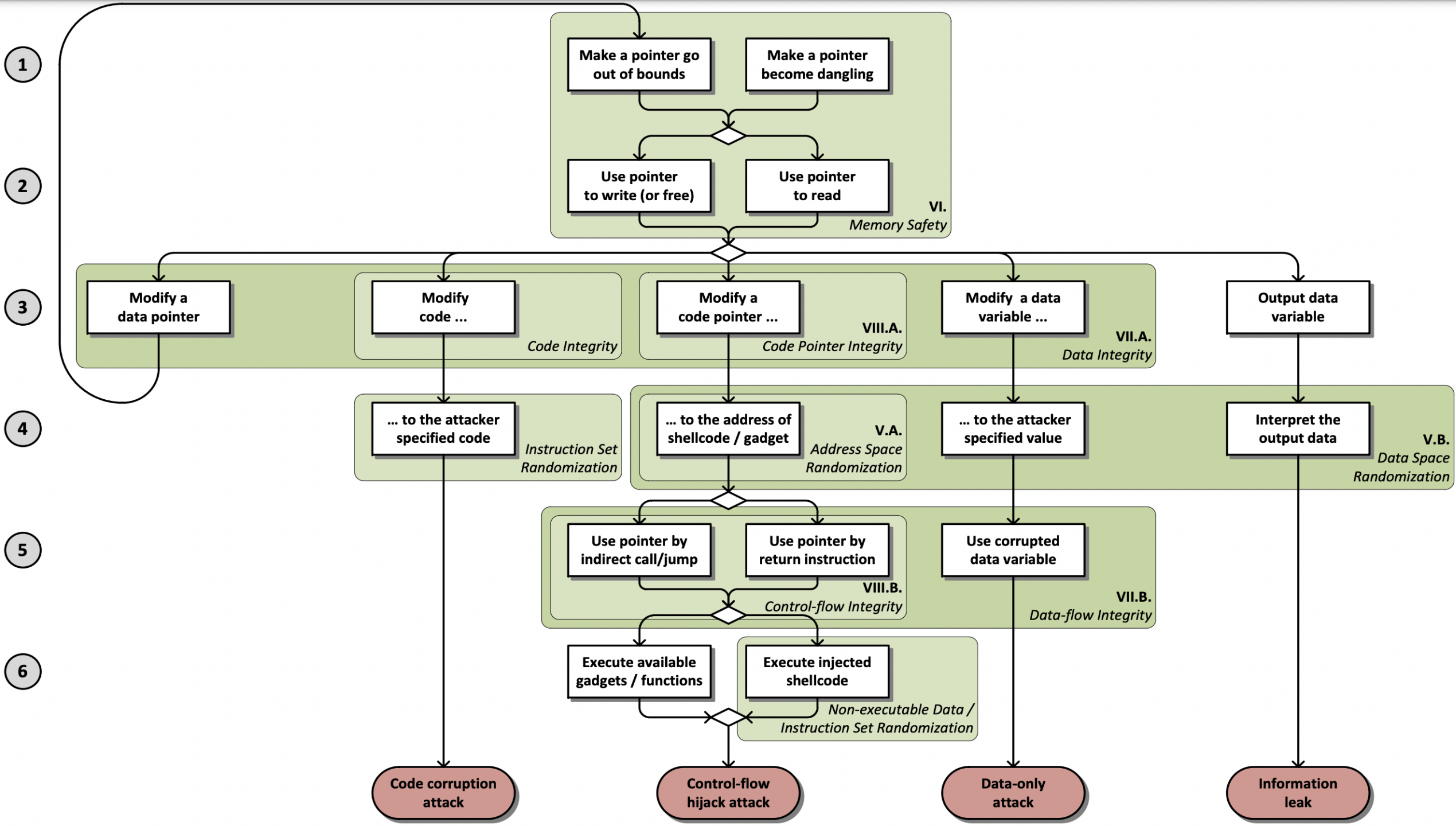
韦韬 博士

蚂蚁集团副总裁兼首席技术安全官
隐语开源社区技术指导委员会主席
北京大学客座教授

韦韬一直致力于让各种复杂系统变得更加安全,发表了 70 多篇国际学术论文,获得中美授权发明专利 30 多项。

内存安全漏洞/内存错误漏洞

- 内存安全漏洞/内存错误漏洞
 - 内存破坏漏洞：更突出内存内容的破坏或篡改
 - C/C++ 等非内存安全语言漏洞
 - 攻击技术
 - Shellcode
 - Return-to-libc
 - ROP
 - 防御技术
 - Stack Canary
 - Data Execution Prevention
 - Address Space Layout Randomization



内存安全漏洞分类

- 越界写/读 (Out-of-Bound Write/Read)
- 缓冲区溢出 (Buffer Overflow)
 - 栈、堆、全局数据缓冲区溢出
- 整数溢出 (Integer Overflow or Wraparound)
- 释放后使用 (Use After Free)
- 失控的资源消耗 (Resource Consumption)
- 空指针 (Null Pointer Dereference)
- 未初始化变量 Uninitialized Variable
-

空间类内存安全漏洞

- 越界写/读 (Out-of-Bound Write/Read)
- 缓冲区溢出 (Buffer Overflow)
 - 基于栈的缓冲区溢出 Stack-based buffer overflow
 - 基于堆的缓冲区溢出 Heap-based buffer overflow
 - 基于全局的缓冲区溢出 Global-based buffer overflow
- 整数溢出 (Integer Overflow)
- 格式化字符串 (Format String)
- 空指针 (Null Pointer Dereference)
- 未初始化变量 (Uninitialized Variable)

时间类内存安全漏洞

- Use-After-Free (UAF) 释放后重复
- Double-Free 双重释放
- Invalid Free 无效释放