第四届全国网络与信息安全防护峰会

用无害碎片制造程序攻击：蒙太奇攻击与程序异常检测

疏晓葵

Virginia Tech

对程序的攻击

独立恶意程序

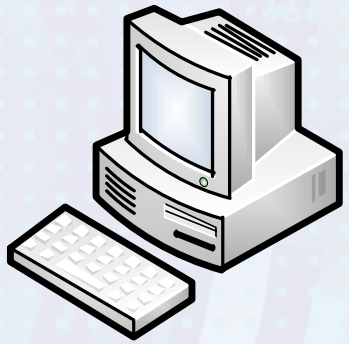
病毒
蠕虫
木马
…

对日常使用程序的攻击

栈溢出
堆溢出
ROP
DoS
在线暴力破解
…

攻击者: 192.168.2.1

受害者: 192.168.2.2



建立恶意网站
192.168.2.1:80

设置后门服务器端
192.168.2.1:4444

访问网站

浏览器获取页面

攻击IE

装载并启动后门

传统防御：基于特征匹配的IDS

特定攻击的特征
CA-2001-26 (IE/IIS vulnerability used by Nimda Worm) GET /scripts/root.exe GET /scripts/..\xc1\x1c../winnt/system32/cmd.exe GET /scripts/..%35c../winnt/system32/cmd.exe

传统防御：基于特征匹配的IDS

（抽象）行为特征

一类Javascript攻击
[Karanth et al. MSR 2010]

unescape()
replace()
new_array()

零日漏洞攻击

Microsoft IE CMshtmlEd::Exec() Use-After-Free Vulnerability

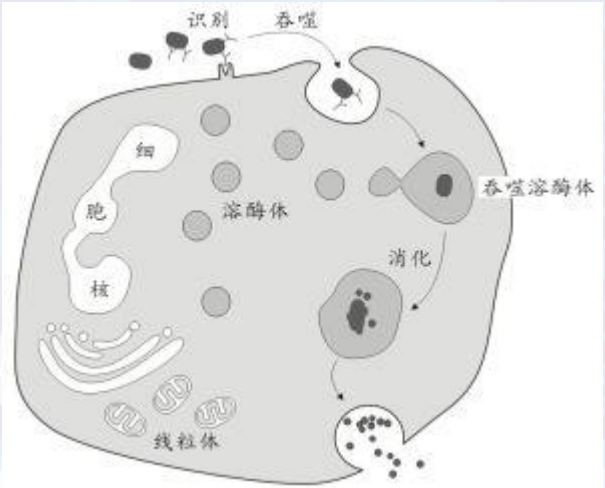
日期	事件
2012.09.14	Eric Romang 发现了这个漏洞
2012.09.16	binjo 公布了漏洞细节
2012.09.17	Metasploit 提供了攻击代码
2012.09.17	Microsoft 向用户提供安全建议
2012.09.21	Microsoft 发布补丁

免疫学的启示

免疫学	特征匹配IDS
人体	操作系统
细胞	程序
病毒	一种对程序的攻击
抗原	攻击的特征
人工免疫	向IDS提供攻击特征

免疫学的启示

免疫学	特征匹配IDS
人体	操作系统
细胞	程序
病毒	一种对程序的攻击
抗原	攻击的特征
人工免疫	向IDS提供攻击特征



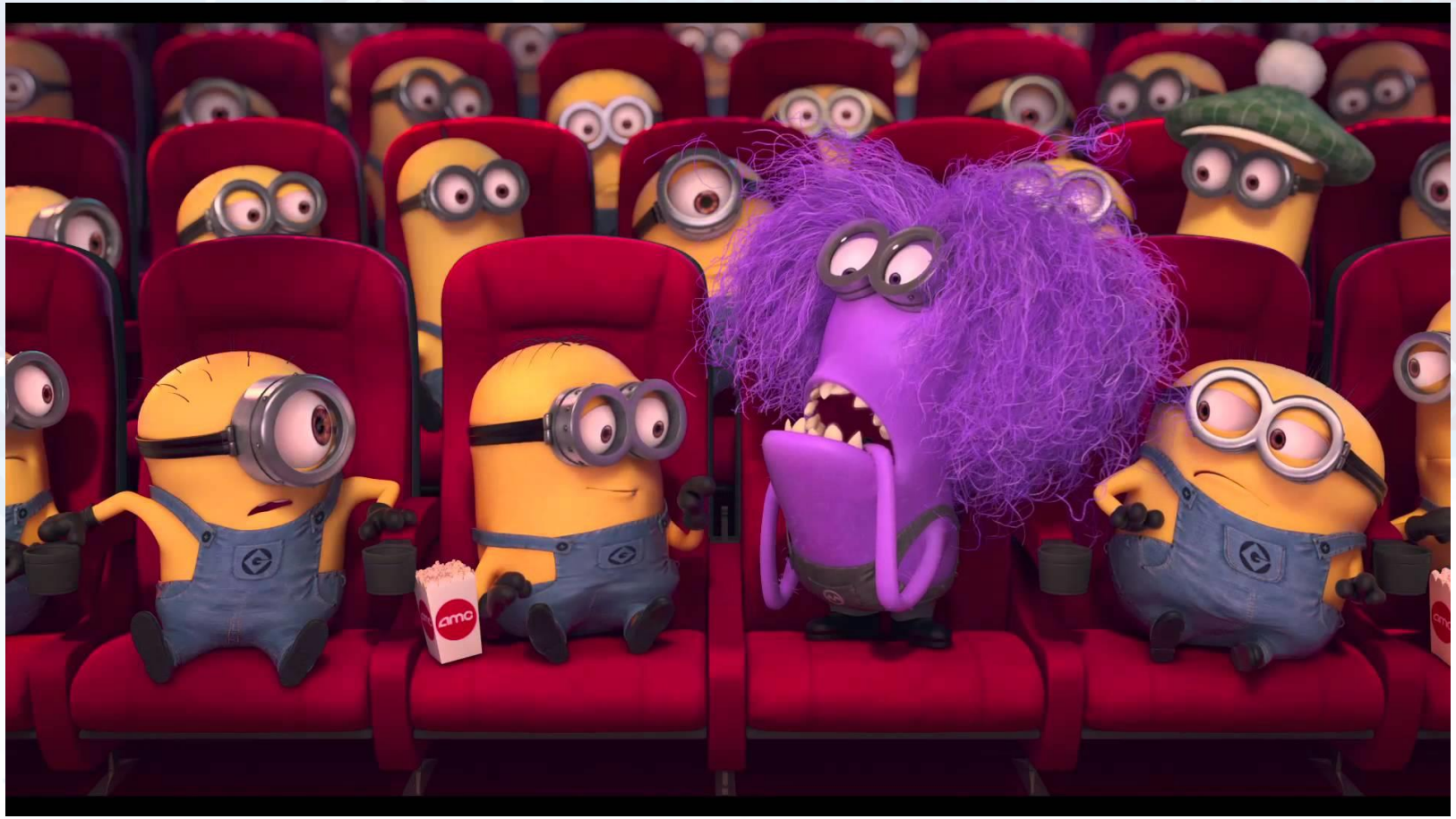
特异性免疫

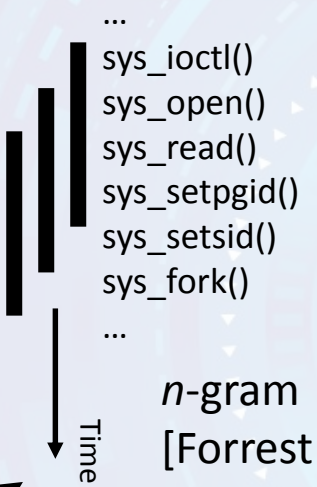
基于特征的IDS

非特异性免疫

基于异常的IDS

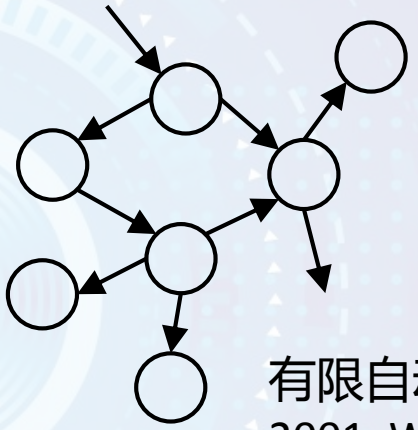
程序异常检测：基于异常检测的IDS





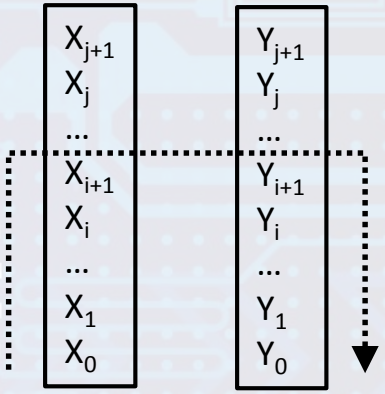
n-gram
[Forrest 1996]

[Forrest 2008]



有限自动机 [Sekar 2001, Wagner 2001]

[Wagner 2002]

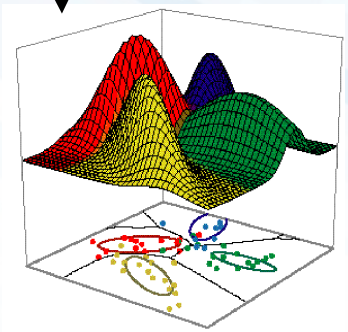


下推自动机 [Feng 2003, Feng 2004, Giffin 2004]

[Feng 2004]

[Sharif 2007]

[Chandola 2009]



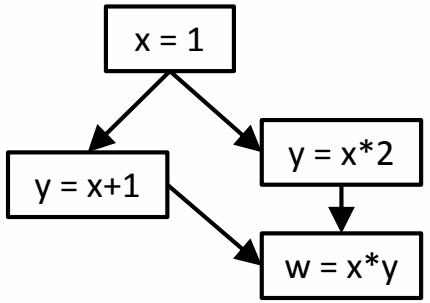
机器学习 [Lee 1998, Mutz 2006, Xu 2015]

Static Program Analysis

+

Dynamic Program Analysis

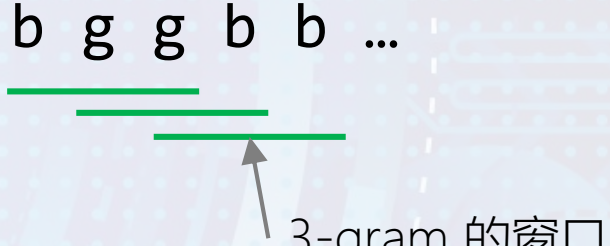
复合模型 [Gao 2004, Liu 2005]



数据流分析 [Giffin 2006, Bhatkar 2006]

基于 n-gram 的程序异常检测

程序运行时的系统调用序列



基于 n-gram 的程序异常检测

程序运行时的系统调用序列

… b g g b b …

3-gram 的窗口

正常的 3-grams:

- bgg
- ggb
- gbb

gram的规则

- ggb 跟随 bgg
- gbb 跟随 ggb

建模及异常检测

基于 n-gram 的程序异常检测

程序运行时的系统调用序列

… b g g b b …

3-gram 的窗口

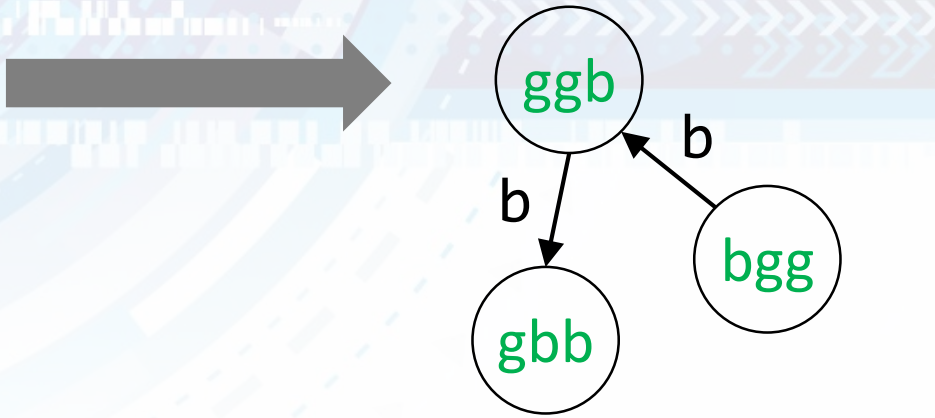
正常的 3-grams:

- bgg
- ggb
- gbb

gram的规则

- ggb 跟随 bgg
- gbb 跟随 ggb

建模及异常检测



有限自动机 (FSA)

基于 n-gram 的程序异常检测

程序运行时的系统调用序列

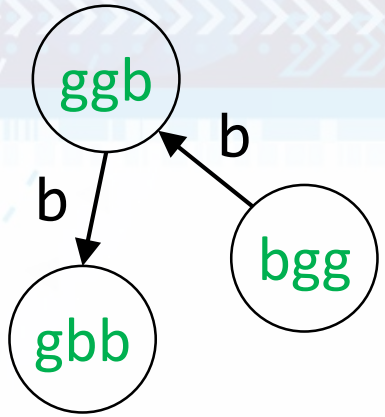
… b g g b b …

3-gram 的窗口

正常的 3-grams:
- bgg
- ggb
- gbb

gram的规则
- ggb 跟随 bgg
- gbb 跟随 ggb

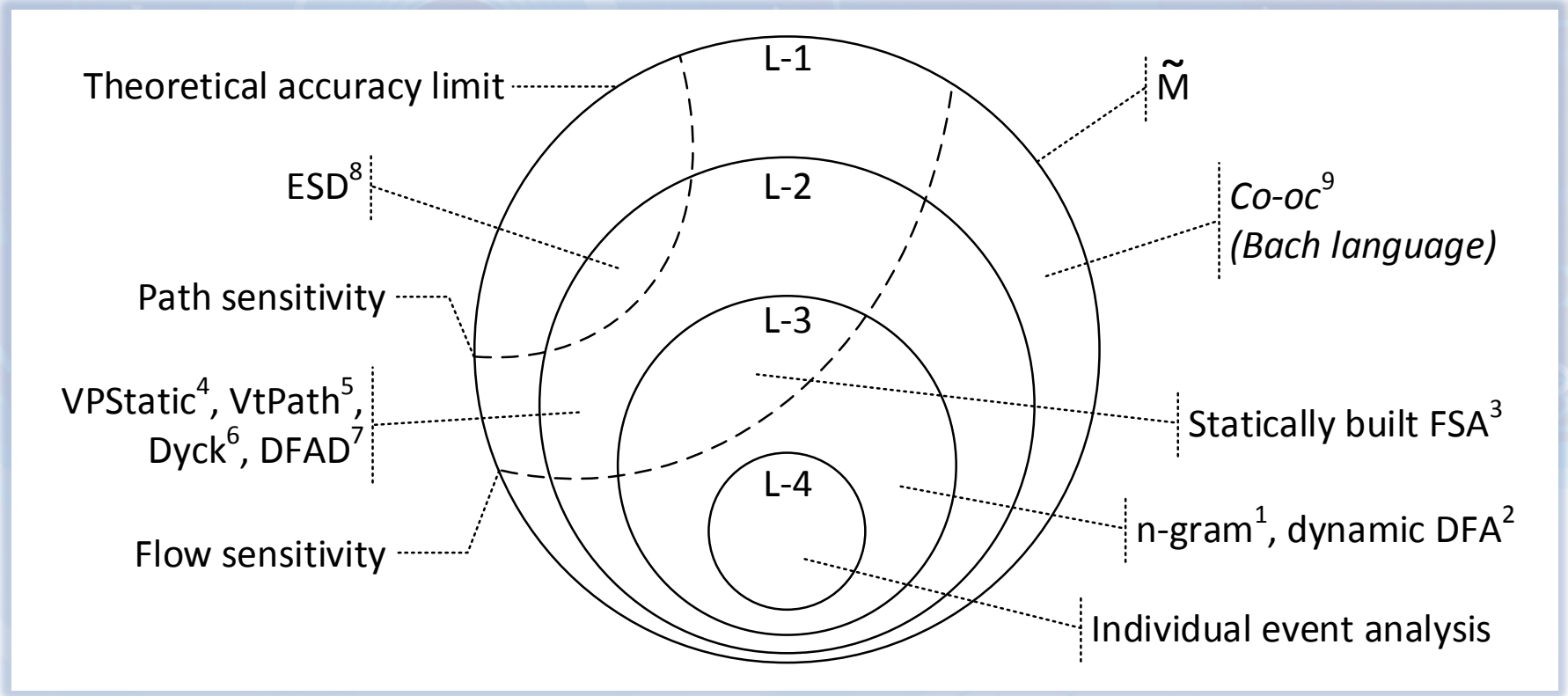
建模及异常检测



有限自动机 (FSA)

正则语言 RE (一种形式语言)

程序异常检测归一化模型 [Shu RAID15]

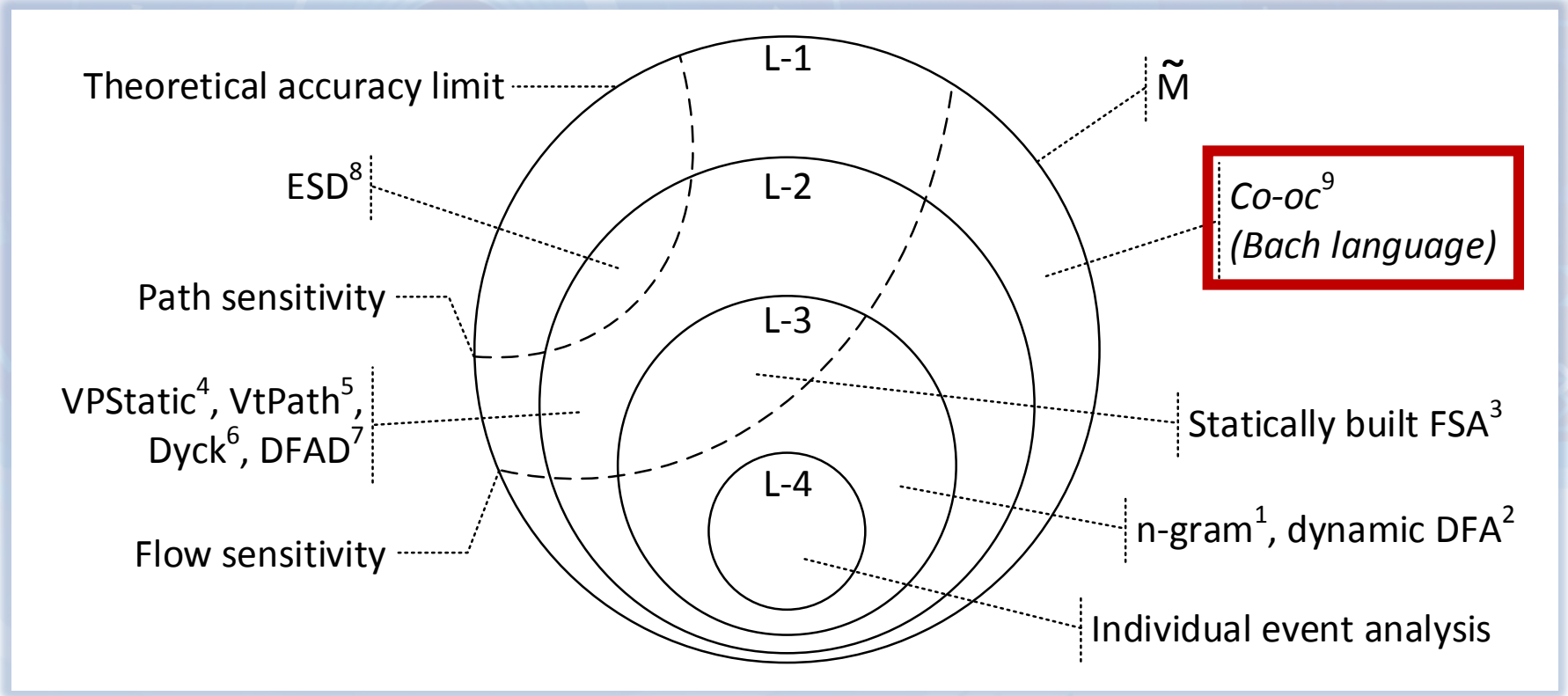


L-1: 上下文相关语言级　　L-3: 正则语言级

L-2: 上下文无关语言级　　L-4: 受限正则语言级

[1][Forrest 1996] [2][Sekar 2001] [3][Wagner 2001]
[4][Feng 2004] [5][Feng 2003] [6][Gin 2004]
[7][Bhatkar 2006] [8][Gin 2006] [9][Shu CCS 2015]

程序异常检测归一化模型 [Shu RAID15]



L-1: 上下文相关语言级　　L-3: 正则语言级
L-2: 上下文无关语言级　　L-4: 受限正则语言级

[1][Forrest 1996] [2][Sekar 2001] [3][Wagner 2001]
[4][Feng 2004] [5][Feng 2003] [6][Gin 2004]
[7][Bhatkar 2006] [8][Gin 2006] [9][Shu CCS 2015]

蒙太奇攻击

一个由正常程序执行碎片构成的运行异常。

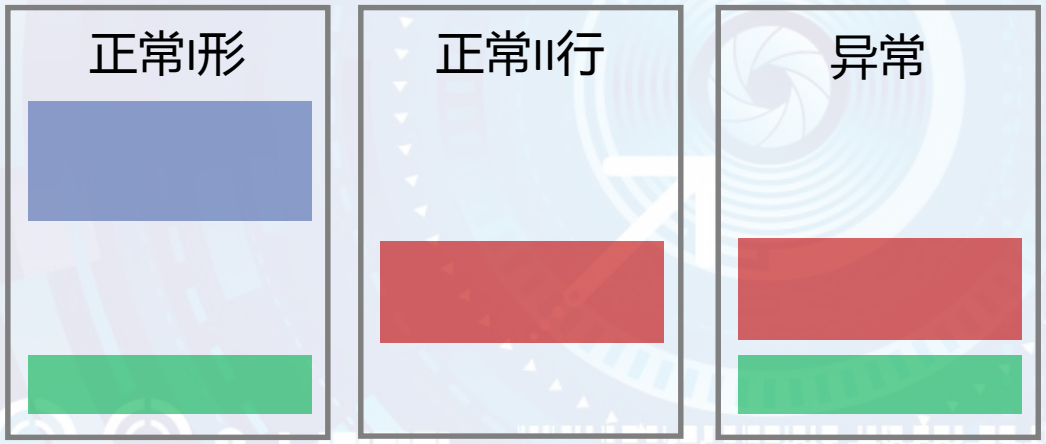
传统异常检测方法等效为一阶自动机，无法分析多个事件的全局联系。

蒙太奇攻击：例一 [Wagner 2002]

```
read() write() close() munmap() sigprocmask() wait4() sigprocmask()
sigaction() alarm() time() stat() read() alarm() sigprocmask()
setreuid() fstat() getpid() time() write() time() getpid()
sigaction() socketcall() sigaction() close() flock() getpid()
lseek() read() kill() lseek() flock() sigaction() alarm() time()
stat() write() open() fstat() mmap() read() open() fstat() mmap()
read() close() munmap() brk() fcntl() setregid() open() fcntl()
chroot() chdir() setreuid() lstat() lstat() lstat() lstat() open()
fcntl() fstat() lseek() getdents() fcntl() fstat() lseek()
getdents() close() write() time() open() fstat() mmap() read()
close() munmap() brk() fcntl() setregid() open() fcntl() chroot()
chdir() setreuid() lstat() lstat() lstat() lstat() open() fcntl()
brk() fstat() lseek() getdents() lseek() getdents() time() stat()
write() time() open() getpid() sigaction() socketcall() sigaction()
umask() sigaction() alarm() time() stat() read() alarm() getrlimit()
pipe() fork() fcntl() fstat() mmap() lseek() close() brk() time()
getpid() sigaction() socketcall() sigaction() chdir() sigaction()
sigaction() write() munmap() munmap() munmap() exit()
```

```
setreuid()
chroot()
chdir()
chroot()
open()
write()
close()
```

蒙太奇攻击：例二



sshd 指示变量改写攻击 [Chen 2005]

```
void do_authentication(...) {
  int authenticated = 0;
  while (!authenticated) {
    if (auth_password(...)) {
      memset(...);
      xfree(...);
      log_msg(...);
      authenticated = 1;
      break;
    }
    memset(...);
    xfree(...);
    debug(...);
    break;
    ...
  }
  if (authenticated) break;
    ...
```

218 call instructions in between

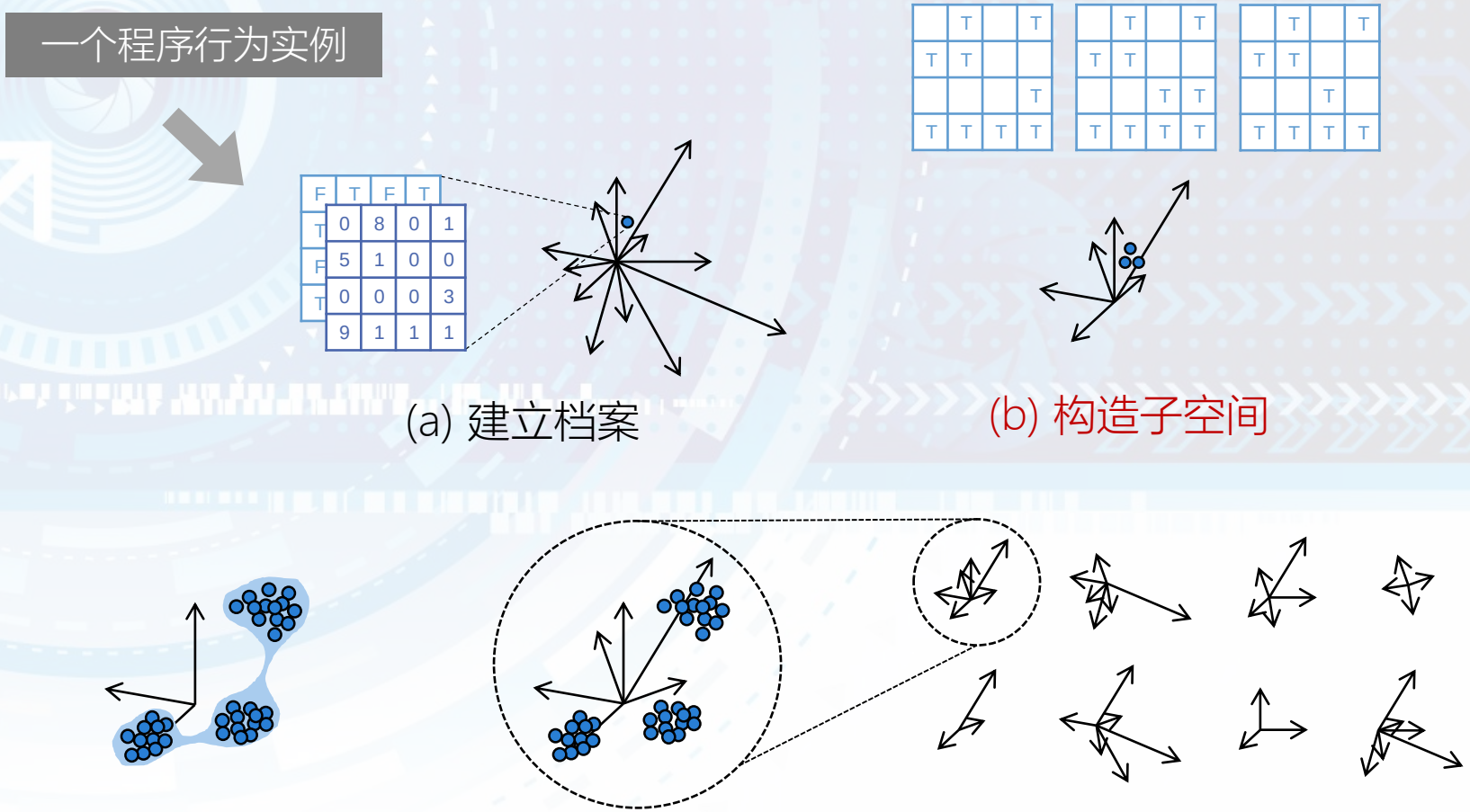
现存方法无法对大尺度下的事件相关性建模

大尺度下程序事件相关性机器学习模型 [Shu CCS15]

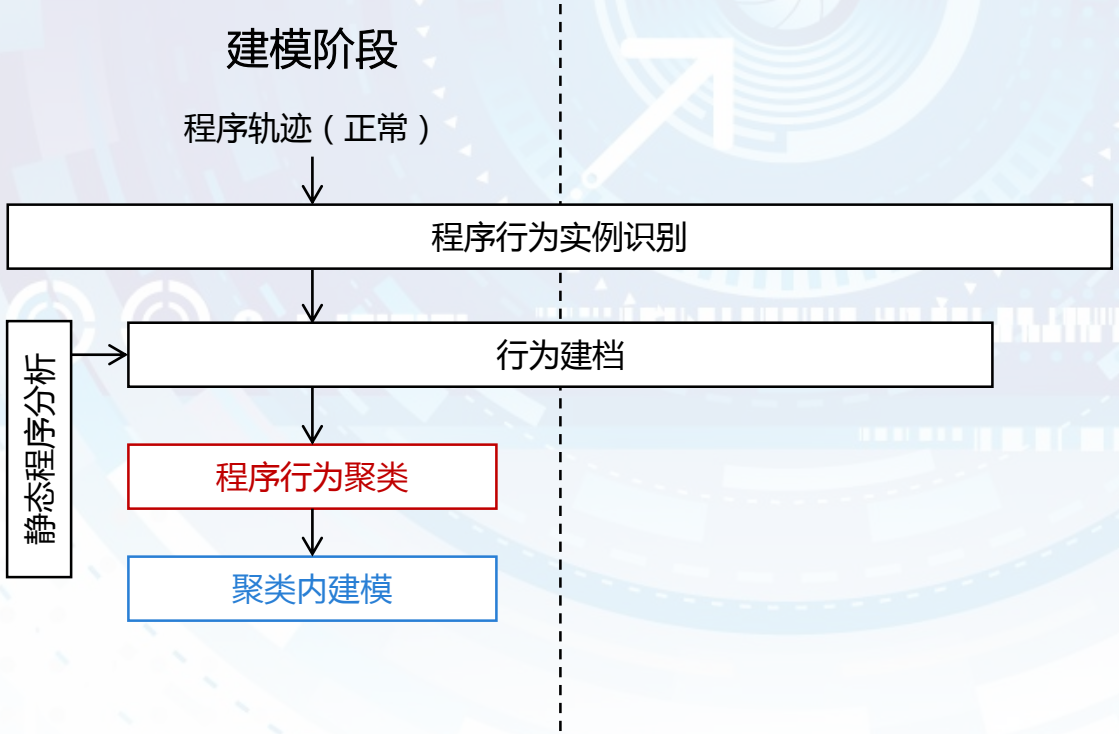
我们提出了一个两段式机器学习模型，为多样化的正常程序行为建模。

聚类间建模
Inter-cluster modeling
事件相关性分析
Event co-occurrence analysis

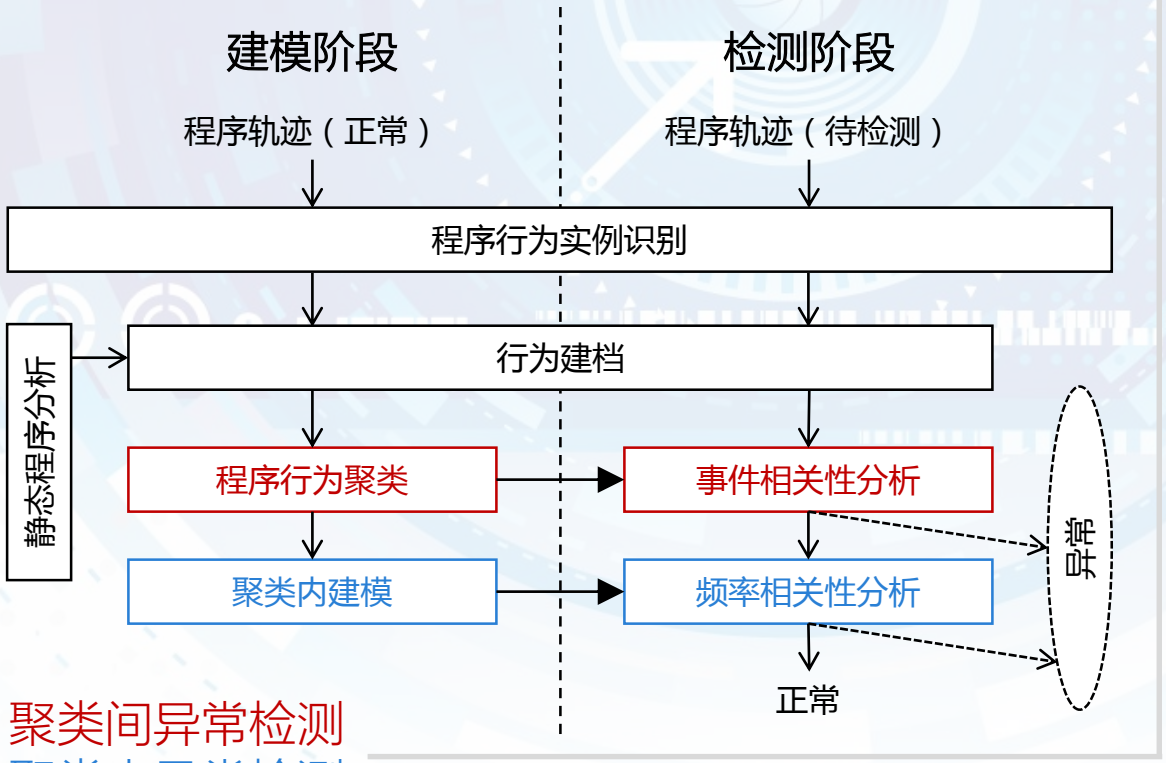
聚类内建模
Intra-cluster modeling
频率相关性分析
Event occurrence frequency analysis



大尺度下程序事件相关性机器学习模型 [Shu CCS15]

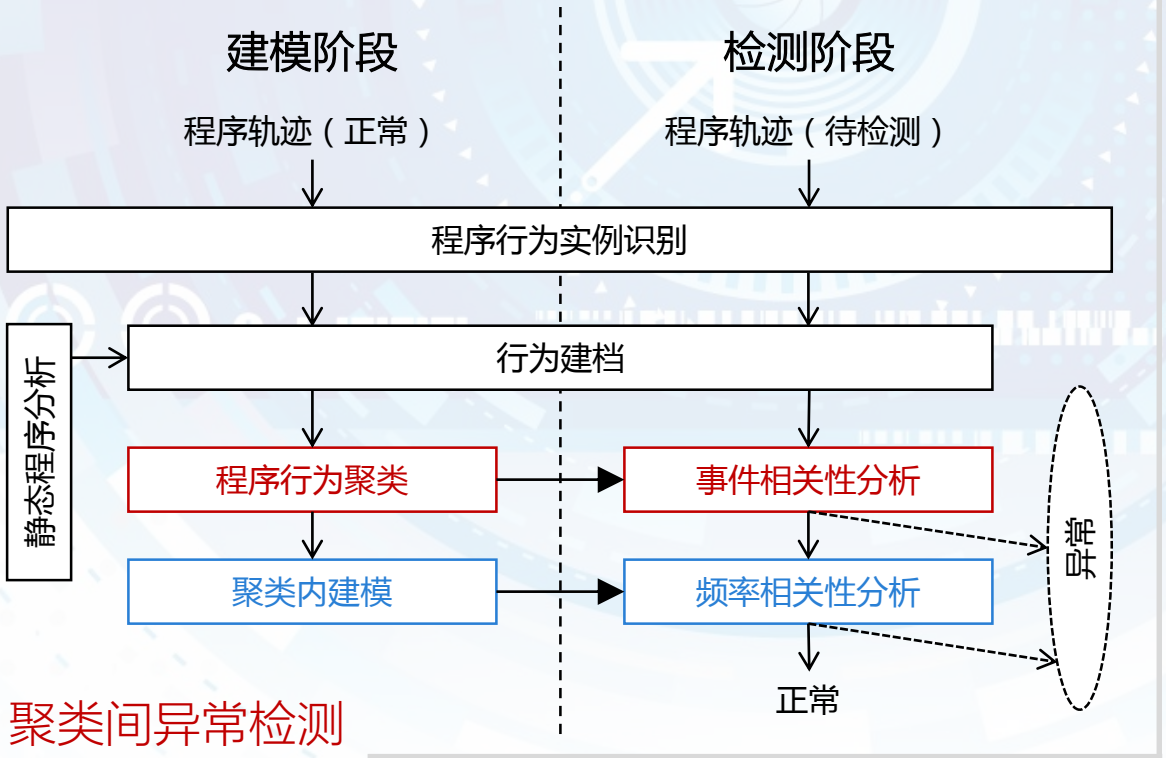


大尺度下程序事件相关性机器学习模型 [Shu CCS15]



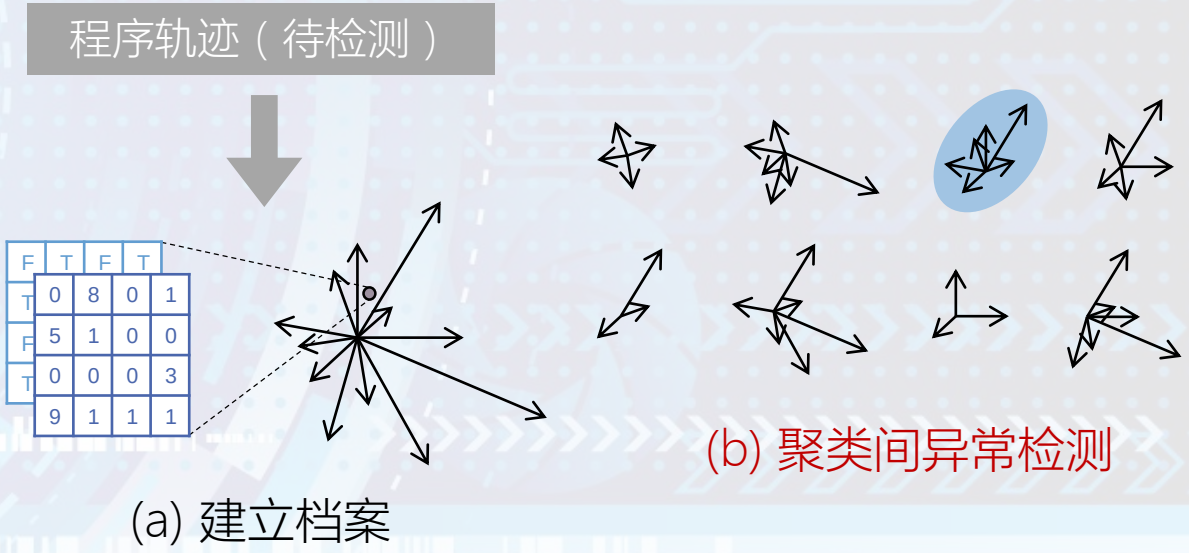
聚类间异常检测
聚类内异常检测

大尺度下程序事件相关性机器学习模型 [Shu CCS15]



聚类间异常检测

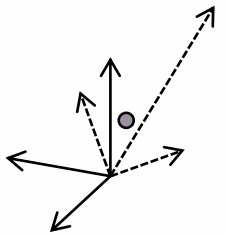
聚类内异常检测



(a) 建立档案

(b) 聚类间异常检测

(d) 聚类内异常检测



(c) 聚类内降维

大尺度下程序事件相关性机器学习模型 [Shu CCS15]

sshd

4800 正常行为档案
平均 34511 事件

指示变量改写攻击

libpcre

11027 正常行为档案
平均 44893 事件

正则表达式拒绝服务攻击

sendmail

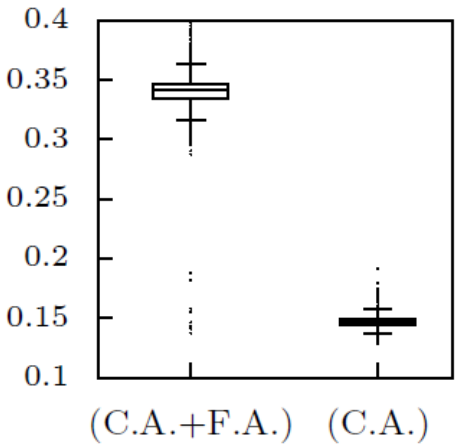
6579 正常行为档案
平均 1134 事件

邮件服务器目录收割攻击

人工合成的异常行为

- 蒙太奇异常
- 不完整执行路径异常
- 高频异常
- 低频异常

行为分析开销



程序异常检测：发展与思考

- 工业界采纳现状
- 程序行为的监测
- 训练模型的完善

总结

- 异常行为检测与攻击特征匹配相辅相成
- 异常行为检测的领域地图 [Shu RAID 2015]
- 蒙太奇攻击与两段式机器学习模型 [Shu CCS 2015]
- 学术界与工业界的交流以及相互帮助

感谢您的关注！

Thank you for your attention