SDN-based solutions for moving target defense network protection

Writer	Panos Kampanakis, Harry Perros and Tsegereda Beyene
Year of Publication	2014
Source	Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014
Link	https://ieeexplore.ieee.org/document/6918979
Notes Link	
Status	Finished
Type	MTD SDN

总结与摘录

1. 抗 TCP 端口扫描

- 工程实现（数据包分类：ACL / 实时分析 / ……）

Algorithm 1 MTD against network reconnaissance

Require: Probabilities $Pr_{SA} < Pr_A < Pr_{PA} < Pr_R < 1$
  hash table $action\_buffer \leftarrow NULL$
  while (new TCP packet p is received) **do**
    if (p is *illegitimate traffic*) **then**
      if (p.dest_port not in $action\_buffer$) **then**
        $r \leftarrow$ random real number $\in [0, 1]$
        store r in $action\_buffer$
      else
        $r \leftarrow$ as in $action\_buffer$
      end if
      switch (r)
       case $r < Pr_{SA}$:
        respond with TCP SYN-ACK
       case $r < Pr_A$:
        respond with TCP ACK
       case $r < Pr_{PA}$:
        respond with TCP PUSH-ACK with random payload
       case $r < Pr_R$:
        respond with TCP RST packet
       default:
        drop silently
      end switch
    end if
  end while

- 特点
  - 优势
    - 产生丰富的混淆流量
    - 混淆结果可调整

      $P_{r_{SA}}$：开放端口

      P_{r_R}：关闭端口

      $P_{r_A}, P_{r_{PA}}$：增加分析难度
    - 防止网络通信过载（SDN programmability）
  - 缺陷
    - 随机混杂的真实数据可能会被攻击者利用
- 性能评价

攻击者代价：

$$C = P_{r_{SA}} * C_{p_l} + (P_{r_A} + P_{r_{PA}}) * C_{p_o}$$

- 混淆结果
  - 探测到随机的开放端口
  - 通信延迟

2. 指纹混淆

- 服务版本 / 应用信息混淆
  - 工程实现：应用代理
  - 特点
    - 优势
      - 为自定义应用程序或代理供应商不支持的应用程序功能提供数据包重组和代理保护
      - 提供自定义代理
    - 缺陷
      - 当服务版本为服务通信必须信息时，该方法无法使用
- OS 指纹混淆
  - 工程实现（数据包分类：ACL / 实时分析 / ……）

Algorithm 2 MTD against OS fingerprinting

```
while (new TCP packet p destined to target is received) do
  if (p is illegitimate traffic) then
    if (p has TCP SYN set) then
      s ← random 32-bit number
      respond with TCP SYN-ACK and s as the seq#
    else
      generate random payload and respond
    end if
  end if
end while
```

  - 特点
    - 优势
      - 产生带有伪造 OS 指纹的混淆流量
      - 增大通信负载，允许攻击者做更多探测
    - 缺陷
      - TCP 分段会导致真实信息泄露 → **重排序可解决**
      - 固定的随机化 TCP 序列号方式或许会被攻击者识别
- 性能评价

  攻击者代价：

  $$C = (1 - P_{r_{ss}}) * C_{sf}$$

3. 随机化

- 随机化主机（Random Host Mutation ，RHM）
  - 工程实现：DNS（虚拟地址映射）+ OpenFlow（通信流 + 地址转换）
- 路由突变（Random Route Mutation ，RRM）
  - 工程实现：OpenFlow
- 应用环境

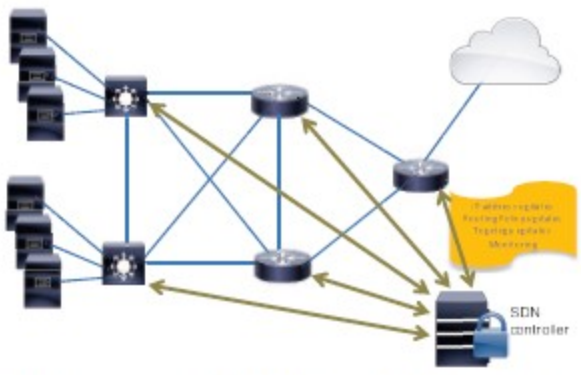
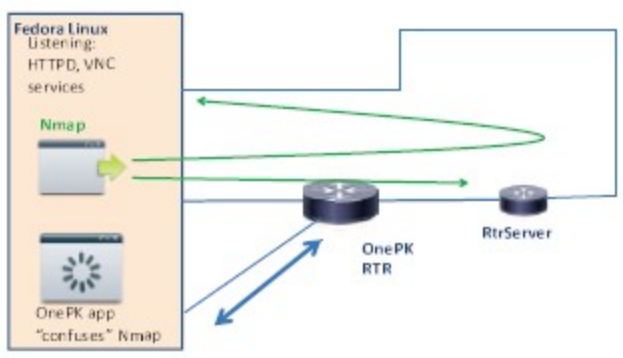


Fig. 2: SDN controlled RHM and RRM architecture

4. 实验复现

- 实验环境
  - virtual router → **onePK**
    - Cisco IOS router (RtrServer)
    - service: HTTP, Telnet
  - virtual machine
    - 32-bit Fedora Linux
    - service: httpd, VNC



- 量化指标（every 1000 scan）
  - Nmap 扫描准确性
  - Nmap 扫描延迟
  - Nmap 通信开销
- 我的观点
  - Nmap 扫本地服务：没考虑到数据包传输过程对指纹的影响