An SDN-Based Fingerprint Hopping Method to Prevent Fingerprinting Attacks

Writer	Zheng Zhao, Fenlin Liu, and Daofu Gong
Year of Publication	2017
Source	Hindawi - Security and Communication Networks, Volume 2017
Link	https://www.hindawi.com/journals/scn/2017/1560594/
Notes Link	
Status	Finished
Type	FPH SDN

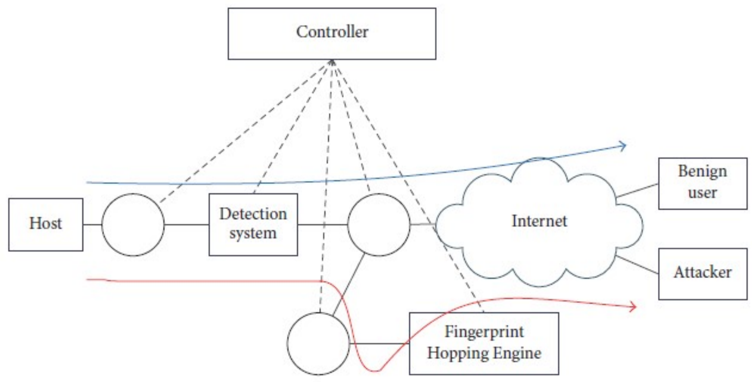
总结与摘录

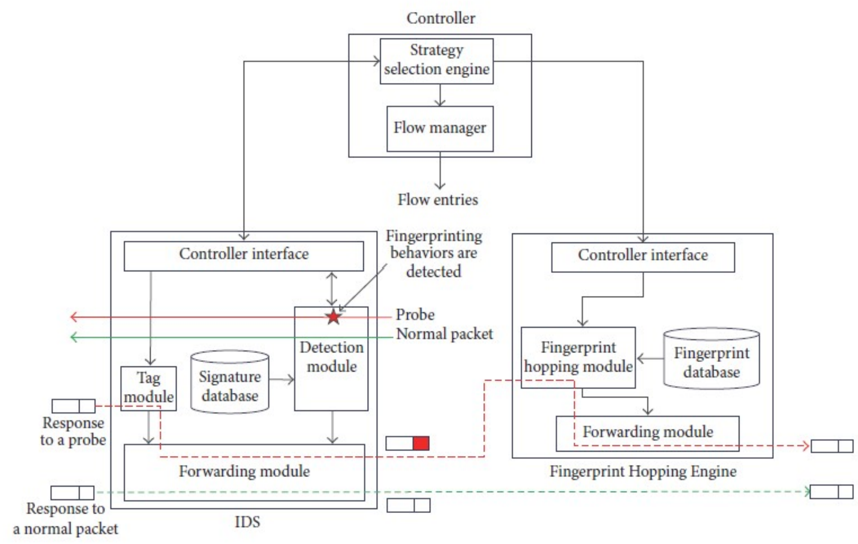
1. 【OS 指纹欺骗】现有研究成果

- **蜜罐 / 蜜网**
  - 类型
    - 基于博弈论
    - 基于 SDN - **HoneyMix**
    - 动态配置
  - 缺陷：当攻击者与目标主机直接通信时防御策略不起作用
- **数据包清洗**
  - 类型
    - 基于博弈论
    - 基于图（static）
  - 缺陷
    - 影响通信速度 → packet header
    - 无法区分通信对象类别
- **基于 MTD 的防御**
  - 类型
    - 改变终端主机的配置
    - 影子网络 → 更改 destination
    - 指纹伪造

2. FPH

- **创新点**
  - 在攻击者获得远程主机 IP 后依然能实施欺骗
  - 实现通信分类
  - 动态、实时的主机 OS 指纹欺骗
  - 改变指纹，不改 destination
  - 提供最优欺骗策略 → 基于博弈论
- **工程实现**
  - 架构设计





- Controller：sender type + 路由管理 + 防御策略
- IDS：恶意探针检测 + 数据包打标
- Fingerprint Hopping Engine：指纹篡改 + 数据包标签删除

- **攻击 - 防御 博弈**（Dynamic Signaling Game）
  - 博弈模型

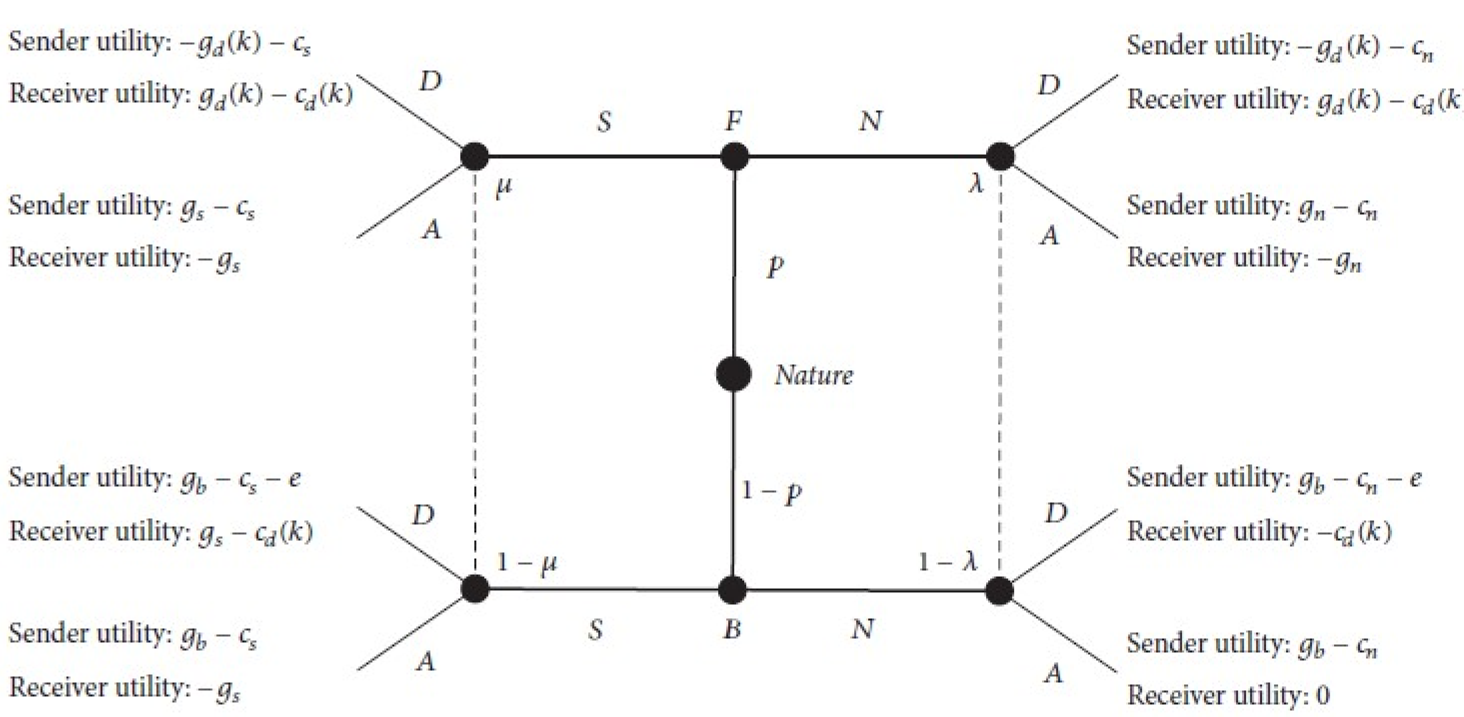


FIGURE 2: Extensive form of the fingerprinting attack and defense game.

【注】

- $g_s > g_n, c_s > c_n$

  $g_d(k) = \alpha \log_u^k, c_d(k) = \beta k - \beta,\ u > 1, \beta > 0, k \in Z^+$
- μ $= P(F|S), 1 - u = P(B|S)$，λ 的计算与之相似（后验概率）
- $Utility = Benefit - Cost$

  - 均衡分析：完美贝叶斯均衡（PBE）

> Perfect Bayesian equilibrium - Wikipedia
>
> In game theory, a Perfect Bayesian Equilibrium (PBE) is an equilibrium concept relevant for dynamic games with incomplete information (sequential Bayesian games). It is a refinement of Bayesian Nash equilibrium (BNE).
>
> W https://en.wikipedia.org/wiki/Perfect_Bayesian_equilibrium

- 均衡条件：$p \geq \frac{c_d(k)}{g_d(k)+g_n}$
- 期望防御效果

  $E_{u_R} = p\alpha \log_u^k - \beta(k-1)$

  $E'_{u_R} = \frac{p\alpha}{k \ln u} - \beta$

  $\therefore k_o = \frac{p\alpha}{\beta \ln u} \rightarrow k_{chosen} = max(k_{min}, \lceil k_o \rceil)$

- 置信度模型

  $p(t) = min(1, \frac{e^{\frac{a_0+\phi(t)}{G}}-1}{e-1}), \ \phi(t) = \frac{1}{\phi}\sum_{i=1}^{t} r_i$

- OS 指纹跳变空间
  - size：$k = |\Xi|$，包括真实指纹

- **防御策略选择算法**

```
Input: t, r_1, r_2, ..., r_t
Output: Strategy
StrategySelect
p* = c_d(k_m)/(g_d(k_m) + g_n)
φ(t) = 0
while communication is going on
    if a new suspicious packet is detected by IDS
        φ(t) = (1/θ) Σ_{i=1}^{t} r_i
        Get p(t) using Eq. (8)
        if p(t) ≥ p*
            Select (D, D) as the strategy of the defender
            Get k = k̃_o using Eq. (14)
            Set up the strategy on the IDS and Fingerprint Hopping Engine
        else
            Select (D, A) as the strategy of the defender
            k = k_m
            Set up the strategy on the IDS and Fingerprint Hopping Engine
end while
return
```

ALGORITHM 1: Strategy selection algorithm.

- **评价指标选择**
  - 通信延迟（ms）→ 与数据包清洗法做对比，**Mininet**
  - 误检情况 → **Nmap** + p0f
    - F：attacker fails to fingerprint the target host
    - NF：attacker falsely identifies the OS
    - Y：attacker succeeds to identify the OS
    - YF：attacker succeeds to identify the OS type but falsely identify the OS version