防火長城的技術與攻防

112-2 資訊安全期末專題報告

40923129L 湯可伊
41047013S 黃紹唐
41047054S 陳柏瑜

大綱

- 引言
- 深度封包檢測 (Deep Packet Inspection)
- P2DPI

引言

GFW 防禦手段

- DNS 汙染
- IP 封鎖
- 主動探測
- TCP 重設攻擊
- 白名單

GFW 翻牆手段

- 關鍵詞修改
- 虛擬私人網路 (VPN)
- 洋蔥路由 (TOR)
- 網頁式代理伺服器 (proxy)

VPN 封鎖

- **深度封包檢測 (DPI)**
- IP 封鎖
- 端口封鎖
- 協議封鎖
- DNS 劫持
- 流量分析
- 主動封鎖

深度封包檢測
(Deep Packet Inspection)

深度封包檢測(DPI)

（Deep Packet Inspection）

傳統封包檢測：只**檢查封包header** -> 封包從哪來、往哪去

深度封包檢測：**檢查整個封包** -> 封包詳細要做什麼

封包被加密：沒辦法直接檢測內容，但可以使用**間接手段**

eg. 流量模式分析、統計特徵提取、TLS/SSL Inspection

現今也有可以同時保證資料隱私的P2DPI

入侵檢測與防禦系統(IDPS)

（Intrusion Detection and Prevention System）

IDPS = IDS + IPS

IDS: 入侵檢測系統, 用於監視網絡流量或系統日誌, **檢測**可能的入侵行為

IPS: 入侵防禦系統, **主動阻止**或防止檢測到的入侵行為

DPI是技術, 常用在這兩個系統中

DPI用在入侵檢測系統(IDS)

在各層使用帶有解析器(parsers)的規則提取模型(rule extraction model), 例如

網路層:來源和目的地的**IP**地址

傳輸層:來源和目的地的**連接埠**(port)和**序號**(sequence number)

應用層:能分析封包**內容**的資訊

解析結果有問題(eg. 檢測到SQL注入攻擊) -> **發出警告**

DPI用在入侵防禦系統(IPS)

用DPI檢查封包 -> 發現有問題 -> **阻止特定流量**或**終止連接**

防火長城使用此方法辨別出不被允許的封包, 並進行封鎖

DPI簽名(DPI signatures):DPI系統中使用的規則, 用於**識別網絡流量中的特徵**(eg. 特定封包結構、協議、關鍵字...), 由各公司自行開發

DPI防火牆

防火牆根據特定的規則對流量進行深度封包檢測(DPI)，並根據檢測結果來決定是**允許還是阻擋流量通過**

例如，**防火長城想封鎖VPN使用者**：

DPI識別到使用VPN(eg. 檢測到VPN協定) -> 限制流量

VPN使用者想避免被封鎖：

- 特殊工具(eg. GoodbyeDPI)，修改封包如 Host -> hoSt
- VPN混淆伺服器，讓封包看起來像沒使用VPN

P2DPI

DPI加密檢驗流量

HTTPS、TLS 、SSH 等加密協定保證了使用者的隱私，卻對 DPI 檢測造成相當的難題。

加密流量會使IDS 等安全服務失明並導致偵測惡意流量極為困難

IDS、IPS 等服務對伺服器運行十分重要，因此出現了保證隱私安全的DPI方法

DPI加密檢驗流量

以下說明以P2DPI為例

利用「key-homomorphic PRF」特性實施

該KH-PRF是具有以下特性的PRF:

$F(k_1, x) \cdot F(k_2, x) = F(k_1 + k_2, x)$

由此可得

$F(k_1,x)^{k_2} = F(k_1 \cdot k_2, x)$

DPI加密檢驗流量

假定三個角色:

S (Sender)

R (Receiver)

M(Middlebox) <- 負責檢查

欲檢查的r(Rules)不應被S或R知道, 否則惡意使用者就可以避開

T(Message) 不應被M知道, 否則洩漏隱私

此場景S, R共享k_{SR}, M擁有k_M

DPI加密檢驗流量

設定規則

M將r以k_M加密得到F(k_M,r)，交與S

S將F(k_M,r)以kSR加密得到F(k_M*k_{SR},r)，交還M

M以k_M還原F(k_M*k_{SR},r)得到F(k_{SR},r)

使用簽章驗證規則來自M

若r不只一條則分別進行

DPI加密檢驗流量

加密驗證

S 將訊息T分割後以k_{SR}加密得到$F(k_{SR}, T_i)$, 交與M
此處以index為salt並Hash, 避免暴露統計特徵
M將$F(k_{SR},r)$加salt並hash後即可進行比對
由於此KH-PRF的輸出是Deterministic的, 因此若$T_i==r$ -> $F(k_{SR},r)== F(k_{SR},T_i)$

參考文獻

1. 林穎佑. "中國近期網路作為探討: 從控制到攻擊." 台灣國際研究季刊 12.3 (2016): 51-68.
2. Wu, Mingshi, et al. "How the Great Firewall of China detects and blocks fully encrypted traffic." 32nd USENIX Security Symposium (USENIX Security 23). 2023.
3. Osborn N. Nyasore "Deep Packet Inspection in Industrial Automation Control System to Mitigate Attacks Exploiting Modbus/TCP Vulnerabilities"
4. Jongkil Kim, Seyit Camtepe, Joonsang Baek, Willy Susilo, Josef Pieprzyk, and Surya Nepal. 2021. P2DPI: Practical and Privacy-Preserving Deep Packet Inspection. In Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security (ASIA CCS '21). Association for Computing Machinery, New York, NY, USA, 135–146. https://doi.org/10.1145/3433210.3437525