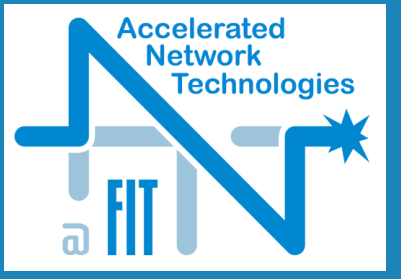
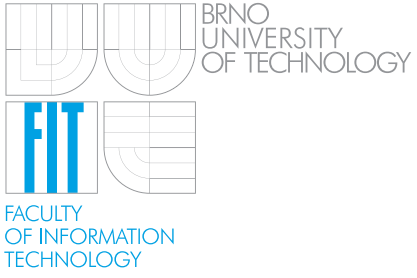
Intrusion Detection Systems
Sekce SIGCOM 2010



Jan Kaštil

Brno University of Technology, Faculty of Information Technology
Božetěchova 2, 612 00 Brno, CZ
www.fit.vutbr.cz/~ikastil



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Obsah

Zařazení

- Metoda detekce anomálií
- Pracuje na úrovni celého síťového provozu
- Neprovádí určení, které toky anomálii způsobily

Vlastnosti metody

- Nevyžaduje trénovací fázi
- Díky specializace na korelované toky dosahuje vysoké přesnosti
- Poskytuje informaci o detekované anomálii

Požadavky metody

- **Nezávislost toků** – Objem přenášených dat je nezávislý na jiných tocích
- **Stacionarity** – distribuce rozdložení toků se nemění v průběhu času

Princip metody

- Data jednotlivých toků jsou rozdělena do košů
- Analyzuje se změna mezi dvěma po sobě jdoucími koši
- Pro každý časový interval se sestaví střední hodnota a rozptyl změn všech toků
- Stanovím nejmenší hodnotu K tak, aby interval spolehlivosti obsahoval 0
- Pokud hodnota K překročí stanovený práh, systém ohlásí anomálii

Poznámky

- Linka nesmí být saturovaná
- Vzorkování nezvyšuje false positive
- Nemusí detekovat anomálie způsobené malým počtem toků

Zařazení metody

- Potlačení DoS útoků
- Využívá prvky infrastruktury místo koncových bodů
- Nedetekuje DoS útoky
  - Zajišťuje každému uživateli spravedlivý podíl na propustnosti

Cíle NetFence

- Spravedlivé sdílení sítě
- Otevřenost novým detekčním metodám
- Škálovatelnost a jednoduchost
- Robustnost
- Incrementální nasazení
- Nesmí záviset na úpravě jiných služeb

Tři typy přenosů

- Požadavky
  - Maximálně 5 procent pásma
  - Používá se pro registraci nové komunikace
  - Pakety mají přiřazenou prioritu
- Datový přenos
  - Přenos samotných dat
- Klasické pakety
  - Používáno routery nepodporujícími NetFence
  - Nejnižší priorita

Princip metody

- Router v paketu informaci, zda zvýšit nebo snížit propustnost linky
- Vysílací router se snaží zvyšovat aditivním způsobem
- Pokud ale nedojde potvrzení, snižuje multiplikativním způsobem

Implementace

- Implementováno a navrženo pro IPv4
- Přidává dodatečnou hlavičku za IP hlavičku
  - Maximálně o velikost 28 bytů
- Hlavička je zabezpečena pomocí MAC
  - Symetrická kryptografie
  - Klíče sdílené pomocí Diffie-Hellman
  - Může přidávat až poslední spolehlivý router
- K zajištění spolehlivé IP se používá Passport
  - Další hlavička za IP

Overhead

- Minimální dokud se nevyskytne problém
- V případě problémů na lince nutno upravovat NetFence hlavičky
- Výpočet MAC

Zařazení metody

- Síťový IDS
- Je založený na popisu zranitelností
- Určený pro vysokorychlostní linky

Co je to zranitelnost?

- Jedná se o chybu v aplikačním programu, kterou může využít útočník
- Vyhledání je obecně nerozhodnutelné

Vzory vs Zranitelnosti

- Vzory neberou v úvahu aplikační protokol
  - Útok může vyžadovat konkrétní hodnotu v několika polích protokolu
  - Protokol může umožňovat zápis jedné věci více způsoby (escape sekvence)
- Zranitelnosti často využívají jednoduchých vzorů

Representace zranitelností

- 2 rozměrné pole
- Každý řádek odpovídá jedné zranitelnosti
- Každý sloupec odpovídá jedné položce protokolu
- Umožňuje implementaci algoritmu výběru kandidátů

Základní princip

- Rozparsujeme aplikační protokol
  - Zajímají nás jen konkrétní hodnoty
  - Velmi zjednodušené parsování
  - Používá vyhledání vzorů a automat popisující protokol
  - Automat lze rozšířit tak, aby parsoval tunelované protokoly
- Vybereme odpovídající zranitelnost
  - Udržujeme si množinu všech možných zranitelností a tu zmenšujeme
  - Každou PDU zpracujeme hned jak dorazí

Slovo závěrem

Identifikace výzkumných oblastí

- Každý článek se zabývá vlastní oblastí
- ASTUTE
  - Poměrně jednoduché operace nad všemi toky v síti
  - Statistické analýzy Flow záznamů v realtime
  - Různé možnosti definice Flow – úrovně agregace
- NetFence
  - Distribuovaná bezpečnost na routerech
  - Doplnění dat do paketu v routerech – Nový protokol
- NetShield
  - Efektivní implementace nového přístupu IDS
  - Spojování výstupů z dříve používaných metod

Společné rysy

- Jedná se o hotová řešení
- Zabývají se vysokorychlostními sítěmi
- Nespoléhají na zabezpečení koncových bodů sítě