Posudek vedoucího diplomové prace

Diplomant: Bc. Martin Nepivoda

Název posuzované diplomové práce: Analýza možností zapouzdření síťových protokolů do aplikačních a metod detekce na firewallech

Posuzovaná práce analyzuje vybrané typy aplikačních protokolů a navrhuje metody, jak zabránit cyklickému zapouzdřování síťových protokolů zpět do aplikačních. Takovéto zapouzdřování je z pohledu bezpečnosti sítě často velmi nežádoucí, neboť umožnuje uživateli obcházet bezpečností pravidla, která jsou v síti stanovena (a implementována na síťových firewallech). Práce se vpodstatě výhradně zabývá malou množinou vybraných aplikačních protokolů -- HTTP, HTTPS, ICMP a DNS, jiné protokoly zcela opomíjí. Výběr protokolů nicméně poměrně přesně reflektuje spektrum protokolů, které jsou uživatelům k dispozici i v sítích s velmi přísnými bezpečnostními pravidly, a tudíž plně pokrývá většinu běžných situací.

Samotný text práce je logicky rozčleněn do dvou hlavních částí. V první se autor textu zabývá možnostmi zapouzdřovaní síťových protokolů rodiny TCP/IP do jednotlivých výše uvedených aplikačních protokolů. Kromě samotného rozboru problematiky vzhledem k danému aplikačnímu protokolu jsou analyzovány a popsány i již existující vybrané implementace.

Druhá část textu se zabývá heuristickými metodami detekce zapouzdřených síťových spojení v aplikačních datech. Jsou popsány a zkoumány dva možné přistupy k takové detekci -- jednak přímou analýzou obsahu paketů na síťové vrstvě, druhak statistickými metodami. V obou částech postrádám hlubší analýzu problematiky adaptivních učících se algoritmů (např. Bayesiánských filtrů). Toto téma je v práci zmíněno pouze okrajově (a implementace se jím nezabývá vůbec), přestože má teoretický potenciál detekovat poměrně sofistikované vzory chování síťového spojení.

Doplňující součástí práce je implementace ICMP filtru podle metody navržené autorem práce. Kód je dobře srozumitelný a efektivní, autor v textu práce uspokojivě prezentuje a interpretuje měření provedená na implementovaném filtru. Programátorská dokumentace je srozumitelná a poskytuje potřebné informace dostatečně detailně.

Práce je napsána v českém jazyce. Po jazykové a estetické stránce nelze textu nic zásadního vytknout.

Domnívám se, že práce splnila cíle stanovené v zadání a doporučuji, aby byla uznána jako práce diplomová.

16.9.2008

Mgr. Jiří Kosina