

Packet Inspection

Jakub “Eremiell” Marek

CryptoParty #3 29/01/2013
CrossCafé

Co je Packet Inspection?

- Zkoumání PDU po cestě
- Shallow Packet Inspection (SPI)
- Medium depth Packet Inspection (MPI)
- Deep Packet Inspection (DPI)
- Rozsah zkoumaných částí

PDU

- 7 vrstev ISO OSI
- Každá vlastní PDU
- PCI + SDU (payload)
- 3 vrstvy “internet”
- 1 vrstva “mezi”
- 3 vrstvy “aplikace”

Net Neutrality

- *“Net neutrality (also network neutrality, Internet neutrality) is the principle that Internet service providers and governments should treat all data on the Internet equally, not discriminating or charging differentially by user, content, site, platform, application, type of attached equipment, and modes of communication.”*
- http://en.wikipedia.org/wiki/Network_neutrality

Pro/Proti

- Listovní tajemství, svoboda
- Spolehlivost a bezpečnost sítě
- Finanční udržitelnost
- Lobby “autorských” svazů
- Spam
- QoS (Quality of Service)
- FUP/EULA

ITU

- International Telecommunication Union
- Obdoba IETF, IEEE
- Při OSN
- “Bridging the Standardization Gap (BSG)”
- Založeno 1865
- 160 standardů/rok (2007)
- Next Generation Networks

ITU u nás

- Ministerstvo průmyslu a obchodu (Admin)
- Český telekomunikační úřad (Regulátor)
- Národní bezpečnostní úřad (Admin Rel)
- Telefónica (poskytovatel)
- FEL ČVUT (univerzita)

ITU-T Y.2770

- Requirements for Deep Packet Inspection in Next Generation Networks
- 10/2012
- Technický standard alá RFC
- Vysoký obsah business slangu/legalese
- Kompletně vlastní terminologie

Reference

- RFC IP (791) IPv6 (2460) IPFIX (5101)
- 8 ITU-T dokumentů
- E.107 X.200 X.731
- Od 2007 5 týkajících se specificky zabezpečením a kontrolou NGN
- Y.1221 Y.2111 Y.2205 Y.2701 Y.2704

Obsah

- Vágní technická specifikace
- Předpokládá vznik celé řady dalších
- Předpokládá DPI na úrovni státu, “odvětví” a poskytovatelů připojení
- Vpodstatě zcela bourá Net Neutrality
- Povoluje odchyťávání a zkoumání payloadu
- Včetně toho, u kterého to specificky nechceme

Pohled z venku

- Mohla by být užitečná, pokud se správně uchopí
- ITU zpracovává tradiční témata lobby
- Ale i tradiční témata userbase
- Jedná se o mezinárodní doporučení
- Nutný soulad s národním a místním právem
- Známe to...