ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ

МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

ЎЗБЕКИСТОН РАДИОТЕХНИКА, ЭЛЕКТРОНИКА ВА АЛОҚА ИЛМИЙ-ТЕХНИКА ЖАМИЯТИ

ИҚТИСОДИЁТНИНГ РЕАЛ ТАРМОҚЛАРИНИ ИННОВАЦИОН РИВОЖЛАНИШИДА АХБОРОТ–КОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИНИНГ АҲАМИЯТИ

Республика илмий-техник анжуманининг

МАЪРУЗАЛАР ТЎПЛАМИ
3-ҚИСМ

СБОРНИК ДОКЛАДОВ

Республиканской научно-технический конференции

ЗНАЧЕНИЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ИННОВАЦИОННОМ РАЗВИТИИ РЕАЛЬНЫХ ОТРАСЛЕЙ Э КОНОМИКИ

ЧАСТЬ 3

6-7 апрел 2017 йил

ТОШКЕНТ – 2017

The political capacity to monitor, mine, and censor for certain data traffic will almost certainly depend on framing. Governments have historically used the language of safety, security, and order to justify blocking communications content. This language of "securitization," a process whereby issues, problems, and phenomena are defined in "security" terms and associated with a "protectionist reflex" can be used to legitimize extraordinary means to solve a perceived problem. While state agents could be responsible for ensuring that content is appropriately mediated, it is possible that the same end – blocking content – could be achieved by a shift towards intermediary liability.

Under such a liability approach "the intermediaries, or companies transmitting or hosting user's communications or other content, are held liable for their user's and customers behavior."

Companies' awareness of their technical capabilities, combined with their (perceived) protection from individual complaints about violations of freedoms of speech and association, can make them the ideal party to which to outsource Internet censorship. Of course, a widespread shift to this liability structure – where ISPs are held accountable for what their subscribers transmit and receive – would constitute a significant transition away from common carrier protections.

Such protections, in theory, immunize ISPs from legal liabilities for what their subscribers transmit so long as the ISPs themselves are not aware of what their networks are carrying. A shift towards ISP liability, however, would effectively mandate awareness of what traffic is being carried. Such a shift might serve to largely formalize already existing practices: today social networking companies, ISPs, journalism sites, and other interactive content communities often censor or block the sharing and posting of content deemed offensive or problematic by the organization in question. Scaling the magnitude of what is blocked or reported to authorities and formalizing the existence of such policies may constitute a quantitative shift but not necessarily a qualitative one in terms of the kinds of actions undertaken.

When simultaneously considering the technical, economic, and political potentialities of deep packet inspection technologies it's helpful to keep in mind that the potential uses of the technology may not necessarily be practically instantiated in real world networking situations. Further, some of the "pure" technical capabilities are infused with the values of control and awareness of the network, and those advocating that the technology be used to meet technical, economic, or political goals may differentially express such values. It is only as I move into the case studies, however, that I will ascertain both the specific drivers and configurations of technologies as well as whether the potentialities of the technology can be, or are being, practically instantiated in the real world.

DPI TIZIMINING TEXNIK TASHKIL ETILISHI

E.B. Normurodov (TATU, 1-bosqich magistranti)

Foydalanuvchilarning ma'lumot uzatish tarmoqlariga qo'yadigan talablari yildan yilga oshib bormoqda. Natijada, Internet provayderlari tashqi kanallar sonini ko'paytirish, yangi qurilmalarni qo'llash orqali tarmoq samaradorligini tushirmaslikka harakat qiladi, katta miqdordagi onlayn videoservislar, P2P tarmoqlaridan ommaviy foydalanish natijasida yangi qurilmalarning resurslaridan nooqilona foydalanishi yuz bermoqda. Bu holat esa operator tomonidan ilovalar trafigini boshqarish zaruratini keltirib chiqaradi. Bugungi kunda trafikni boshqarishning asosan quyidagi usullaridan foydalaniladi:

- ✓ MAC-adreslar yoki VLAN asosida;
- ✓ Uzatuvchi va qabul qiluvchilarning IP adreslari asosida;
- ✓ TCP va UDP portlari raqamlari orqali;
- ✓ Proksi-serverlarda domen nomlarini cheklash asosida.

Bu usullar OSI modelining faqatgina transport sathigacha ishlashga mo'ljallangan tarmoqlararo ekranda amalga oshirilishi mumkin. DPI texnologiyasini tadbiq qilish internet va

boshqa ma’lumot uzatish tarmoqlarida turli saytlarga ulanishni cheklash, tarmoqqa ruxsatsiz kirishni cheklash, tarmoqni virusli dasturlar va keraksiz axborotlardan tozalash, tarmoqlardagi turli noqonuniy reklamalarni kesib tashlash, xavfsizlikka tahdid soluvchi turli axborot paketlarini tutib qolish, bir so’z bilan aytganda provayder o’z tarmog’ini to’liq nazorot ostiga olish imkonini beradi. DPI tizimlari traffik klassifikatsiyasini to’g’ri va aniq amalga oshirishi uchun turli internet dasturlarini aks ettiruvchi katta hajmdagi signaturalar bazasi bilan ta’minlanishi lozim. DPI tizimiga qo’yiladigan muhim talablardan yana biri, u paketni ma’lumot uzatish kanali tezligida tekshirishi kerak. Bu esa tarmoqda bo’lishi mumkin bo’lgan yo’qotishlarni va yuklamalarni oldini oladi. DPI (Deep Packet Inspection) tizimi paketlarni OSI modelining 2-sathidan 7-sathigacha nazorat qilish imkoniyatiga ega.

DPI tizimi imkoniyatlari quyidagilardan iborat:

- ✓ turli ko’rinishdagi statistik ma’lumotlarni yig’ish;
- ✓ turli mezonlar asosida trafikni filtrlash (bunda odatiy “IP-adres+port”ga domen nomlari va protokollari ham qo’shiladi, masalan P2P yoki Skype trafiklarini aniqlash imkoniyati mavjud);
- ✓ foydalanuvchilarga turli darajada xizmat ko’rsatish;
- ✓ hujumlardan himoya qilish. Code Red, NIMDA , SQL Slammer, DoS, DDoS kabi tarmoq hujumlaridan himoyalash.

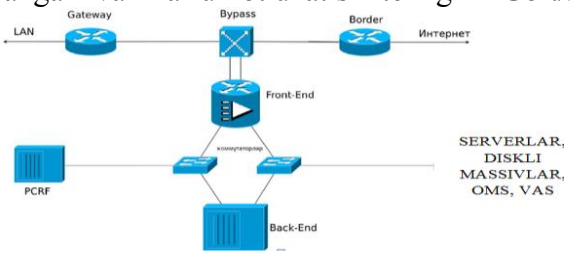
DPI tizimi aloqa operator tarmog’ining chegarasiga qo’yiladi. DPI texnik vositalari quyidagi komponentlardan tashkil topgan:

- ✓ Bypass;
- ✓ Front-End qurilmasi;
- ✓ Back-End qurilmasi;
- ✓ PCRF-serveri (Policy and Charging Rules Function);
- ✓ komponentlar orasida aloqani ta’minlaydigan kommutatorlar;
- ✓ serverlar (qo’shimcha);
- ✓ disk massivlari (qo’shimcha);
- ✓ VAS qurilmasi (Value Added Services – spam va viruslar tekshiruvi) (qo’shimcha). Umumiy sxemasi 1-rasmdagi ko’rinishga ega.

Birinchi bo’lib tarmoqqa Bypass, keyin esa unga Front-End ulanadi. Bypass ikkita ishlash rejimiga ega:

1. Himoya. Trafik to’g’ri liniyaga o’tib ketadi va Front-End qurilmasiga uzatilmaydi.
2. Ishchi. Trafik Front-End qurilmasiga uzatiladi.

Front-End ishdan chiqqanda, uning portlariga ulangan kabel shikastlanganda, DPI texnik vositalari elektr ta’minotidan uzilib qolganda Bypass himoya rejimiga o’tadi. Bypass elektr yoki optik turda bo’lishi mumkin. Elektr Bypass relega asoslangan bo’lib, mis simlar ulashga mo’ljallangan va ma’lumot uzatish tezligi 1 Gbit/s gacha bo’ladi.



1-rasm. DPI tizimining tipik sxemasi

Optik Bypass bir necha afzalliklarga ega: ma’lumot uzatish tezligi 10 Gbit/s gacha, trafikni akslantirish imkoniyati yuzaga keladi (trafik to’g’ri kanal bo’yicha ketayotganda uning nusxasi Front-End ga uzatiladi, trafik bilan hech qanday amallarni bajarish imkoniyati mavjud bo’lmasada, statistika olib borish mumkin bo’ladi). Front-End qurilmasida paketlar OSI modelinig kanal sathidan amaliy sathigacha tahlil qilinadi. Operator tarmoq

samaradoligini oshirish maqsadida alohida turdagi trafikni cheklab qo'yishi mumkin. SHuningdek, tarmoqdagi turli hujumlardan himoyalanish ham Front-End qurilmasida bajariladi. Back-End qurilmasida barcha qoidalar majmuasi, yig'ilgan ma'lumotlar statistikasi, signaturalar, akslantirish va qayta yo'naltirish marshrutlari yig'iladi.

PCRF-serverining asosiy vazifasi foydalanuvchi-qoida raqami mosligini saqlash. Front-End qurilmasi PCRF-serveriga abonent identifikatorini uzatadi, PCRF-serveri javob tariqasida Front-End qurilmasiga qoida raqamini uzatadi, Front-End qurilmasi bu qoidaning tavsifi yuzasidan Back-End qurilmasiga so'rov yuboradi.

THE TECHNICAL POSSIBILITIES OF DPI

A.S. Umarov (assistant, TUIT)
A. A. Makhamadjonov (master of TUIT)

Network administrators are concerned with the functioning of the network itself: are security incidents logged and kept to a minimum? Do network policies simultaneously ensure the functioning of the network and meet users' expectations and needs? Are the network's nodes appropriately configured to address congestion? Deep packet inspection helps administrators improve network security, implement access requirements, guarantee quality of service, and tailor service for particular applications. Each of these functions is dynamic, insofar as the technology can utilize layered rule sets and is incorporated within a broader networking assemblage to dynamically react to changes in the network. As a result of DPI's penetration into packet transfers, combined with its potentialities, the technology can be helpful in daily and long-term network operations.

DPI was initially meant to offer network providers improved intrusion detection and prevention mechanisms that could recognize and respond to contemporary threats. To respond to emerging threats, DPI appliances are reconfigurable and can scale to monitor high volumes of traffic and to provide logging and anomaly detection. Logging establishes a pattern of known behavior and lets the system (and system administrator, if they examine the logs) examine traffic 'offline'. Offline analysis facilitates a granular analysis of the traffic because it needn't occur in real time, thus mitigating some of the technical challenges associated with in-depth analysis of data packets while maintaining high data-transit speeds. As a result of logging traffic, systems and administrators can 'learn' how to sub-classify network traffic within applications. To make analysis process a bit clearer, consider a process of logging unencrypted HTTP, or web browser, traffic.

It is also possible to use logging-based learning to develop expected use-patterns for individual users and applications and to send notifications to administrators if deviations from the norms are detected. Such deviations may indicate that a known client's credentials are being used by a third-party to access the network, based on suspicious or deviant data transmissions and receptions, or that an application has been infected with malware. Because DPI systems afford high levels of control, if a particular detection signature is too 'chatty' – if a signature is being identified regularly but is uninteresting to the network administrator – the DPI system can be set to either ignore or more carefully monitor the signature in question. A more careful monitoring schema might narrow down the parameters of the inspection, such as shifting from monitoring for all encrypted communications across a corporation to monitoring for encrypted communication in specific business units that are not expected to engage in secure communications. Alternatively, the system might be set to avoid establishing a 'normal' activity pattern for authenticated 'guest' accounts because the logged in user(s) regularly changes, though the equipment could still watch for anomalous application behavior.

More generally, as a component of an integrated security processes, DPI can examine inbound and outbound data traffic and flag packets that warrant a more sustained analysis of their contents. This flagging might happen when the device cannot positively identify the