Internetes megfigyelés mély csomagvizsgálattal (DPI)

Az internet-, és telefonszolgáltatók, valamint a távközlési vállalatok mindig is képesek voltak hálózatuk felügyeletére, monitorozására. Az olyan információkat, hogy ki kivel kommunikál, milyen weboldalakat látogat, és milyen szolgáltatásokat vesz igénybe, a számlázáshoz, a hálózatirányításhoz és a vállalati marketinghez használták. A mély csomagvizsgálat (DPI) névre hallgató technológia azonban az interneten zajló kommunikáció tartalmának az elérését is lehetővé teszi a szolgáltatók, a titkosszolgálatok és a kormányok számára. Ez olyan, mintha a postán felbontanák és elolvasnák a leveleinket, esetenként akár változtatnának is a tartalmukon, vagy törölnének belőlük, esetleg szándékosan nem kézbesítenék ki őket.

A mély csomagvizsgálat képes figyelemmel kísérni minden internetes tevékenységünket és kommunikációnkat. Kezdve attól, hogy mit olvasunk el, milyen honlapokat látogatunk meg, milyen videókat nézünk meg, illetve, hogy milyen szavakra keresünk rá a böngészőben, egészen addig, hogy kikkel és mit kommunikálunk e-mailben, egyéb üzenetküldő rendszereken vagy a közösségi oldalakon. A mély csomagvizsgálatot végző alkalmazások meg-

Hogyan működik a mély csomagvizsgálat?

Az információ, amit Ön küld vagy fogad az interneten, igen összetett folyamaton megy keresztül, miközben jó pár számítógépen áthalad.

Az internet által összeköttetésben álló számítógépek feldarabolják az Ön által küldött üzenetet, és kisebb egységekre, úgynevezett „csomagokra" bontva továbbítják azt. Ennek köszönhetően az információ vagy üzenet könnyebben halad át az interneten. Amikor a csomagok megérkeznek célállomásukhoz, itt puzzle módjára összekapaszkodnak, hogy az üzenet ismét teljes legyen. Hasonlóan a postán feladott levelekhez, minden ilyen csomagon található egy címke, amit „címzésnek" hívnak. Ezen van feltüntetve, mi ez a csomag, mit tartalmaz, kitől származik és hova tart. A csomagban belül található a „rakomány", ami tulajdonképpen az üzenet tartalma.

Minden csomagnak több rétege van, amelyek különböző információkat tartalmaznak az üzenetről. Ezek a rétegek az orosz matrjoska babához hasonlóan egymásba ágyazódnak. Az internetszolgáltatóknak ezek közül néhány réteget mindenképpen meg kell vizsgálni, hogy a csomagokat megfelelően továbbítani tudják. Az esetek többségében elég, ha csupán a címzést ellenőrzik (egy postai levél esetén ez lenne az, ami a borítékra van írva), és nem szükséges átnézniük az üzenet tartalmát, vagyis a mélyebb rétegeket. Ezt nevezzük felszíni csomagvizsgálatnak. Ezzel szemben a mély csomagvizsgálat alkalmazása során a címke mellett az üzenet összes többi rétegét, vagyis a teljes tartalmát átvizsgálják.

A csomagokat olyan számítógépes algoritmusokkal ellenőrzik, amelyek az üzeneteket pásztázva speciális adatfajtákra, információkra keresnek. Az okos térfigyelő kamerákról szóló részben már volt szó algoritmusokról, vagyis olyan számítások sorozatairól, amelyek rendezik és elemzik az adatokat. Ugyanilyen algoritmusokat használ a mély csomagvizsgálat is, csak más módon.

A mély csomagvizsgálat során az algoritmusok úgy vannak kialakítva, hogy bizonyos „kulcsszavak" után kutassanak, hasonlóan ahhoz, mint ahogy Ön is rákeres kulcsszavakra az internetes böngésző keresőjében. Az, hogy a mély csomagvizsgálat pontosan milyen adatok után kutat, azon múlik, hogy ki és milyen célból futtatja azt. A keresett kulcsszavak kapcsolatban állhatnak például bűncselekményekkel, vagy egyéb gyanús tevékenységekkel, esetleg egy új számítógépes vírussal, vagy akár azzal, hogy valaki egy adott terméket megvásárolt-e.

nyitják és átvizsgálják az üzeneteket, hogy kiszűrhessék közülük azokat, amelyek veszélyes tartalmakat hordoznak. Éppen ezért ahhoz, hogy a mély csomagvizsgálat az Ön internetes kommunikációját is érintse, nem szükséges, hogy Ön gyanúsított legyen. Ez a technológia képes ugyanis lehallgatni és elolvasni minden üzenetet, ami az internetszolgáltató hálózatán áthalad.

1.1 Milyen céllal fejlesztették ki a mély csomagvizsgálatot?

A mély csomagvizsgálatot eredetileg azért fejlesztették ki, hogy kiszűrjék a vírusokat, illetve az egyéb rosszindulatú szoftvereket (malware), amelyek kárt okozhatnak a számítógépes hálózatban. Manapság a mély csomagvizsgálatos üzenetelemzéssel már nemcsak a vírusokat lehet megfékezni, hanem az interneten kifejtett rossz szándékú, veszélyes vagy törvényellenes tevékenységek is leleplezhetők.

Az összes eszköz, ami a mély csomagvizsgálathoz szükséges, az internetszolgáltatók birtokában van, akik így ellenőrzésük alatt tudják tartani az internet teljes működését mind lokálisan, mind regionálisan, mind pedig országos-, illetve nemzetközi szinten. Ezek a vállalatok saját céljaikra szánták ezt a technológiát, azonban hamar ráébredtek, hogy komoly haszonra is szert tehetnek ennek eladásából. Idővel más vállalatok, például védelmi ipari cégek is bekapcsolódtak a módszer fejlesztésébe. Így mára a mély csomagvizsgálati technológiának komoly piaca lett.

1.2 Hogyan használják a mély csomagvizsgálatot?

Európában a mély csomagvizsgálatot legálisan csak nagyon korlátozottan lehet használni: a jelenleg hatályos jogszabályok szerint az internetes forgalom „szűrésére", vírusok és rosszindulatú programok (malware-ek) elhárítására lehet hadba állítani. Ezenfelül segítheti az internetszolgáltatókat a hálózatukban zajló adatforgalom irányításában. Azonban a mély csomagvizsgálat arra is képes, hogy az internetes kommunikációk teljes tartalmát elemezze. Amikor erre használják, alkalmas olyan speciális bűncselekmények leleplezésére is, mint amilyen például a gyermekpornográfia terjesztése. Ez azonban jogi szempontból meglehetősen ellentmondásos, mivel jelenleg nincs érvényben olyan jogszabály, amely a mély csomagvizsgálatot megfelelő részletességgel szabályozná. Ennek az az oka, hogy amikor a kommunikációs technológiákra vonatkozó európai jogszabályokat megalkották, még nem létezett a mély csomagvizsgálati technológia. Az Európai Bíróság és az Európai Adatvédelmi Biztos értelmezése szerint a meglévő törvények az on-line kommunikáció „szűrését" csak korlátozott mértékben teszik lehetővé. Új törvények kidolgozására van szükség, amelyek a mély csomagvizsgálat lehetőségeit részletesen leírják és megfelelően szabályozzák.

Emiatt jelenleg Európában legálisan még nem megengedett a mély csomagvizsgálat alkalmazása a kommunikációk általános figyelésére, a szerzői jogok internetes megsértésének felderítésére, a politikailag kényes tartalmak vagy a célzott reklám letiltására, bár maga a technológia már alkalmas lenne ezekre a feladatokra. Az európai törvények védik a bizalmas kommunikációt. A mély csomagvizsgálat sértené az emberi jogok európai egyezményét is, hiszen indokolatlan, tömeges, nem célzott megfigyelést jelent, mivel a komputerek közötti információforgalom minden kis bitjét képes leolvasni.

Más a helyzet az Egyesült Államokban, ahol ez a terület nincs szabályozva, és sok cég használja is a módszert reklámok célzott terjesztéséhez. Amennyiben Ön például Gmail™ vagy Yahoo™ postafiókkal rendelkezik, az üzenetei szinte biztosan áthaladnak az Egyesült Államokon, és átesnek mély

csomagvizsgálaton. 2013 nyarán került nyilvánosságra, hogy az amerikai Nemzetbiztonsági Ügynökség (NSA), és a brit hírszerzés, a General Communications Headquarters (GCHQ) minden bizonnyal tömeges megfigyelést végző programokat használt.

Egyelőre megválaszolatlan az a kérdés, hogy a mély csomagvizsgálatot milyen módon lehet észlelni, korlátozni vagy kontrollálni. Habár a szabályozás folyamatosan igyekszik felvenni a tempót a technológiai fejlődéssel, szinte lehetetlen felmérni, hogy milyen mértékben használják ezt a módszert. Bármelyik Ön által küldött üzenet megfordulhat a világ bármely pontján mielőtt célba ér, és eközben akár több országban is átvizsgálhatja annak tartalmát mély csomagvizsgálattal egy internetszolgáltató vagy egy kormány titkosszolgálata. Szinte lehetetlen megmondani, mi történik. A szabályozás hiányában az interneten „vadnyugati" állapotok uralkodnak, ahol a kormányok és vállalatok kedvükre használhatják ki a zavaros helyzetet.

Csupán annyit tudhatunk biztosan, hogy világszerte különféle intézmények használnak mély csomagvizsgálatot. Időnként internetszolgáltatók, marketingcégek, rendőri szervek, illetve állami titkosszolgálatok élnek ezzel a módszerrel. Az amerikai titkosszolgálatok Edward Snowden számítógépes szakember leleplezése nyomán 2013-ban nyilvánosságra került tömeges állami megfigyelésein túl is ismert a mély csomagvizsgálat néhány felhasználása: egy részük kereskedelmi felhasználás, más részük a közbiztonsági és nemzetbiztonsági területhez kapcsolódik.

1.2.1 Kereskedelmi célú felhasználás

- **Hálózati biztonság:** üzenetek átvizsgálása abból a célból, hogy kiderüljön, nem tartalmaznak-e vírusokat, illetve, hogy kiszűrjék a felhasználók közötti nagyméretű fájlmegosztást
- **Viselkedés-alapú internetes reklám:** adatok gyűjtése az üzenetekből azzal kapcsolatban, hogy valaki milyen termékeket részesít előnyben. Európában ez nem engedélyezett, de az Egyesült Államokban sok vásárló kedveli, és ott szabad is. Lehetővé teszi a vásárlók számára, hogy egyszerűbben hozzájussanak a nekik megfelelő termékekhez és szolgáltatásokhoz
- **Digitális jogok védelme:** üzenetek átvizsgálása abból a célból, hogy leleplezzék az illegális fájlmegosztást, illetve a szerzői jogok megsértését

1.2.2 Közbiztonsági és nemzetbiztonsági használat

Bűncselekmények állami megfigyelése: a mély csomagvizsgálat alkalmas bizonyos bűncselekmények felderítésére, bár alkalmazása jogilag vitatott. Ilyen bűncselekmények például:

- a számítógéprendszerek ellen irányuló, vagy számítógéppel elkövetett jogsértések (pl. gyermekpornográfia terjesztése)
- rasszista tartalmak megosztása, rasszista indíttatású fenyegetések
- felbujtás terrorcselekmények elkövetésére, vagy azok szervezése
- népirtást vagy emberiség elleni bűntetteket helyeslő tartalmak megosztása

Cenzúra: sokan gyanítják, hogy diktatórikus rezsimek világszerte használnak mély csomagvizsgálatot politikai ellenfeleik félrevezetésére, megtévesztésére. Az egyik amerikai hadiipari vállalat, a NARUS, amely egyébként a Boeing leányvállalata, eladta a mély csomagvizsgálati technológiát a líbiai kormánynak, amit az fel is használt az arab tavasz során, hogy megakadályozza az ellenzéki vélemények terjesztését. Nem tudni, honnan, de Irán is hozzájutott a technológiához. Irán a mély csomagvizsgálattal nemcsak megfigyeli az állampolgárait és nemcsak cenzúrázza az internetes tartalmakat, hanem félrevezetés céljából meg is változtatja azokat. Kína hasonló módon alkalmazza ezt a technológiát. Felmerülhet tehát a kérdés, vajon Európában is alkalmaznak-e internetes cenzúrát.

1.3 Hogyan növeli biztonságunkat?

A mély csomagvizsgálat javíthatja az információbiztonságot és elősegíti a bűnözés elleni harcot azzal, hogy képes kiszűrni és blokkolni a 7.2.2 pontban felsorolt veszélyes, ártalmas vagy bűnözésre utaló üzeneteket.

Bár a mély csomagvizsgálat nem képes megelőzni a súlyos bűncselekményeket, amelyekre ezek az üzenetek utalhatnak, lehetővé teszi azok felderítését, és bizonyítékokat szolgáltathat egy nyomozásban. Megakadályozni is képes viszont a számítógépes vírusok terjedését és az internetes bűnözés más formáit.

1.4 Milyen problémákat vet fel?

A mély csomagvizsgálat a következő problémákat veti fel:

1. A mély csomagvizsgálat mindent lát.
   - Képes minden üzenetet és bizalmas tartalmat elemezni, miközben azok áthaladnak a hálózaton, ami annyit jelenti, hogy mély csomagvizsgálat mellett az elektronikus kommunikáció többé nem maradhat magánügy.
   - Az a tudat, hogy a kommunikáció már nem bizalmas többé, erőteljes öncenzúrát válthat ki, ahol az emberek félnek nyíltan kommunikálni egymással, és feladják a szabad önkifejezést.
   - Fontos lenne, hogy a mély csomagvizsgálat alkalmazása szigorúan legyen szabályozva, mivel az használója számára jelentős hatalmat biztosít.
2. A technológia gyorsabban fejlődik, mint a szabályozás.
   - Nincsenek világos szabályok arra, hogy a mély csomagvizsgálatot mire szabad használni és mire nem.
   - A gyakorlatban a mély csomagvizsgálat alkalmazásának a módja kizárólag a technikát használó tisztességén múlik. Ezt a technológiát bármire fel lehet használni, a számítógépes vírusok felderítésétől a politikai elnyomásig.
   - Olyan országokban, ahol az állam és az internetszolgáltató vállalatok között szoros a kapcsolat, könnyen előfordulhat, hogy az állam hozzáfér a polgárok teljes elektronikus kommunikációjához.
3. Nehéz megállapítani, hogy pontosan ki és hol alkalmaz mély csomagvizsgálatot:
   - Az egész világra kiterjedő egységes jogi szabályozásra lenne szükség. Adatvédelmi hatóságok már egy ideje világszerte felhívásokat fogalmaznak meg a privátszféra nemzetközileg elfogadott minimumkövetelményeinek a meghatározására.
   - A mély csomagvizsgálat szabályozását egy olyan nemzetközi intézményre kellene bízni, amely ténylegesen képes megbüntetni azokat, akik visszaélnek vele.
4. A mély csomagvizsgálat hatékonysága megkérdőjelezhető.
   - Miközben a mély csomagvizsgálatot végző számítógépek a potenciálisan veszélyt jelentő összes üzenetet kiszűrik, nem képesek valódi szövegértelmezésre vagy rangsorolásra, így felvetődik a téves értelmezés lehetősége, és az a probléma, hogy esetleg ártatlan emberekből is gyanúsítottak válhatnak.
   - Több szakértő kétségbe vonja a mély csomagvizsgálat hatékonyságát az illegális tartalmak leleplezésében.

IMPRESSZUM

*Ez a tájékoztató a **SurPRISE** (**Sur**veillance **PRI**vacy and **SE**curty) európai kutatási projekt keretében készült, amelyben a Medián Közvélemény- és Piackutató Intézet is részt vett, és amelyet az Európai Unió Kutatási és Technológiafejlesztési Hetedik Keretprogramja támogatott. A 2015 januárjában lezárult SurPRISE project fő célkitűzése az volt, hogy összegyűjtse az európai polgárok véleményét az új biztonsági technológiákról.*

További részletes információk a projektről a Medián honlapján (www.median.hu) és a kutatás nemzetközi honlapján találhatók: http://surprise-project.eu/

Szerzők: Kirstie Ball (Open University Institute, UK)

Szerkesztő fordító: Márta Szénay (Medián)

Dizájn: Zsolt Bartha (Medián)

Medián, 2015. január