Biztonságos kommunikáció peer-to-peer hálózat segítségével

Lopusni Gábor
IV. évf. programtervező informatikus

Témavezető: Dr. Alexin Zoltán egyetemi adjunktus

SZTE TTIK Szoftverfejlesztés Tanszék

Az Internet egyre nagyobb szerepet játszik az emberek, különösen a fiatalok életében. A közösségi média egy olyan színtér, amelyben a felhasználók életük kisebb-nagyobb eseményeit megörökítik, sőt a világ elé tárják. Nem gondolnak arra, hogy ezek a tartalmak hová kerülnek, hogyan dolgozzák fel őket.

Az Interneten nyilvánosságra hozott adatokat ipari módszerekkel dolgozzák fel erre alapított társaságok, de akár állami hatóságok is, például az adóhivatal. A begyűjtött információkat rendszerezik, kereshető adatbázisokba rendezik. Amennyiben a polgárok személyes adatokat hoznak nyilvánosságra, akkor megkönnyítik a róluk szóló információ feldolgozását, kiszolgáltatják a magánéletüket ismeretlen érdeknek.

Akkor sem lehetünk biztonságban, ha jelszóval védett portálokon tároljuk az adatainkat. Az állami hatóságok jogi eszközök segítségével, mesterségesen létrehozott hátsó ajtókon keresztül jutnak hozzá az adatainkhoz, anélkül, hogy erről tájékoztatást kapnánk. Nem feltétlenül olyan adatokról van szó, amelyek kiszolgáltatása számunkra jelentős kockázatot okozhat, elvégre a privát fotók, emlékek kiszivárogtatásából komolyabb hátrányunk nem származhat, de azért mégsem látnánk szívesen fényképeinket egy-egy idegen weboldalon, miközben a tudtunk szerint biztonságban vannak. Az általunk a hétköznapokban használt kommunikációs eszközök, lehet ez szöveg alapú, vagy kép-és hang alapú szolgáltatás, mint például a Skype, vagy Facebook Messenger, ugyancsak lehallgatásra, megfigyelésre kerülnek. Ráadásul a megfigyelés nem célirányosan egy szűk csoportra, vagy személyre irányul, hanem az összes felhasználóra kiterjed.

A kockázatokat akkor sem tudjuk teljesen kizárni, ha tudjuk, hogy az Internetes szolgáltatást nem figyelik meg a hatóságok, és nincsenek benne mesterséges hátsó ajtók. Az ilyen oldalakat is megtámadhatják kiberbűnözők (hackerek), akik rövidebb-hosszabb idő alatt megtalálják a módját annak, hogyan jussanak hozzá a tárolt tartalomhoz.

A fenti kockázatok kivédésére született meg, néhány olyan szoftvereszköz, amelynek a használatával nagyobb biztonságban érezhetjük magunkat, nem kell attól félnünk, hogy bárki látja, vagy hallja, amit beszélünk. Ezek az eszközök end-to-end titkosítást használnak, amely azt jelenti,

hogy kizárólag a két fél számára értelmezhető az elküldött üzenet és csak az ő eszközük használatával mehet végbe ez a kommunikáció. A titkosításra több mód is rendelkezésre áll, történhet kulcs alapján (szimmetrikus, asszimetrikus), illetve szteganográfia alkalmazásával. Ez a kommunikációs módszer nem gátolja meg azt, hogy fizikailag lehallgatásra kerüljön egy beszélgetés, azt sem teszi lehetetlenné, hogy megfelelő erőforrások segítségével feltörjék az üzeneteket. Ugyanakkor a lekötött erőforrások miatt jelentősen megdrágítja, megnehezíti a minden polgárra kiterjedő adatgyűjtést. A Tudományos Diákköri Konferencia dolgozatomban ezekkel a megvalósításokkal, titkosítási módszerekkel, illetve a személyes adataink biztonságát érintő fenyegetésekkel, jogvédő kezdeményezésekkel és indítványokkal fogok foglalkozni.

Az end-to-end titkosítást megvalósító szoftverek közül dolgozatomban a Freenet, ZeroNet, I2P, RetroShare, OmniShare rendszerekbe fogok betekintést nyújtani. Későbbi terveim között szerepel az, hogy a ZeroNet rendszerhez egy újabb kommunikációs modult készítek. Az felsorolt programok peer-to-peer hálózaton keresztül kommunikálnak egymással, kivéve az OmniShare esetében, amely egy felhő alapú tárhely szolgáltatás és egyedi titkosítási eljárást használ. Peer-to-peer hálózaton azt értjük, hogy nincs egy központi szerver, amelyen keresztül a kliens adatot cserél, hanem a kliensek maguk kommunikálnak egymással, azaz decentralizált. Minél több fél kapcsolódik a hálózathoz, annál magasabb a biztonsági szint. Minden résztvevő csak a szomszédjait ismeri, számukra feltérképezhetetlen az egész hálózat. A programok feladata, hogy az üzenetek a küldő és fogadón kívül mások számára elérhetetlenek és értelmezhetetlenek legyenek. Ezt titkosító algoritmus felhasználásával érik el. Ezeket egy zárt hálózatként is elképzelhetjük, mivel rejtve maradnak a világháló elől, külsőleg hozzáférhetetlen, egyedül olyan személy tudja használni, akinek az eszközén jelen vannak a megfelelő szoftverek, miután felcsatlakoztunk az általunk kiválasztott hálózatra biztonságosan kommunikálhatunk. Nem vonhatók felelősségre a szerzők, akik ezeket az eszközöket elkészítették, és nem kényszeríthetik őket adatok közlésére, mivel ezek az információk számukra is rejtve maradnak. Az ismertetésre kerülő szoftverek több különböző programozási nyelven íródtak, mindegyikük nyílt forráskódú projekt keretében elérhető a fejlesztőknek vagy a felhasználóknak. A Freenet és I2P Java, a ZeroNet Python, a RetroShare és OmniShare pedig C++ nyelven készültek.