A Brit törvényjavaslat az üzenetküldö alkalmazások 'BCC'-zésére, a magánéletet veszélyezteti

PCLinuxOS Magazine – 2022. január

Írta: Paulo Garcia, tanársegéd, Carleton University
Utánnyomás a The Conversation-ből
Creative Commons Attribution/No derivatives 4.0 licenc alapján

A „fantom protokoll" kifejezésre Tom Cruise híres kasszasiker filmje ugorhat be, de itt a brit kormány Government Communications Headquarters (GCHQ) nevű szervezetének új javaslatáról van szó.

A GCHQ az USA National Security Agency brit megfelelője és a javaslat célja, hogy a bűnüldöző szerveknek módjuk legyen belehallgatni titkosított kommunikációkba (mint például, ami a WhatsApp-on folyik).

A brit kormány nem először veszi célba a titkosított kommunikációt: 2017-ben Amber Rudd, az akkori belügyminiszter, kezdeményezte a végpontok közötti titkosítás betiltását, azt állítva, hogy „egyszerű embereknek" nincs szükségük rá. Rudd megjegyzése a modern kommunikáció működésének teljes hiányát mutatja.

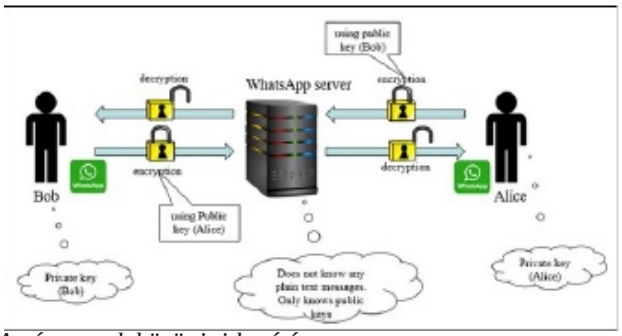
A nem hivatalosan fantom protokollnak hívott javaslat sokkal súlyosabb támadás a privát szféra ellen, biztonsági retorikával leplezve annak technikai, személyi és társadalmi következményeit. A GHCQ-nak írt nyílt levélben 47 aláíró – köztük az Apple, a Goole és a WhatsApp – sürgette a terv elvetését.

Hogyan működik a végpontok közötti titkosítás?

A kormányjavaslat szerint „még csak hozzá sem kell nyúlni a titkosításhoz" a fantom protokoll alkalmazása érdekében. A végpontok közötti titkosítás úgy működik, hogy minden felhasználónak készítenek egy publikus és egy privát kulcsot. A szöveget a publikus kulccsal titkosítják és csak a privát kulccsal olvasható és vice versa.

Így, ha Bob és Aliz csevegni akar, megosztják egymással a publikus kulcsukat és megtartják a privátot maguknak. Bob Aliz kulcsával titkosítja az üzeneteket (így csak Aliz tudja megfejteni) és Aliz Bob publikus kulcsával titkosítja az üzeneteket.

Csoportos csevegésnél Aliz, Bob és Jill között, Aliz minden üzenetét titkosítja Bob publikus kulcsával (Bob számára) és Jill publikus kulcsával (Jill számára). Az alkalmazás jelzi, hogy minden üzenetnek két címzettje van. Ez azt jelenti, hogy az üzenettovábbító szerverek csak a publikus kulcsokat és a titkosított szöveget látják: nem tudják visszafejteni a szöveget, még a bűnüldöző szervek kérésére sem.



A végpontok közötti titkosítás

Fantom a gépen

A fantom protokoll azzal kerüli meg a problémát, hogy javasolja a bűnüldöző szervek hozzáadását a csevegéshez láthatatlan részvevőként. Aliz a Bobbal folytatott csevegésében minden üzenetet duplán titkosítana, egyszer Bob publikus kulcsával és egyszer a bűnüldözés publikus kulcsával. Aliz nem tudna arról, hogy a bűnüldözők hozzáférnek a csevegéséhez.

A tálalás, hogy a műveletre csak jogi felhatalmazás birtokában kerülhetne sor és csak akkor, amikor elegendő bizonyíték van annak igazolására, jól hangzik, de a fantom protokoll teljesen figyelmen kívül hagyja a fantom felhasználó érdekében a szoftver módosításának számos technikai következményét.

Meg kellene változtatni azt, ahogy a csevegő alkalmazások a felhasználók között egyeztetik a kulcsokat, tovább bonyolítva, ami potenciális biztonsági sérülékenységet eredményez.

Az a követelmény az alkalmazásokkal szemben, hogy elrejtsenek részvevőket, aláássa az azonosítási folyamatot, új potenciális sérülékenységet okozva és rombolva a felhasználók szolgáltató iránti bizalmát.

Hátsó bejáratot is létrehozhat, amit az csevegő alkalmazások maguk is kihasználhatnak – például egy cég alkalmazottja egy munkatársát akarja megfigyelni. Ez maga is hibapontot hoz létre: rosszindulatú támadó megbütyköli a csevegő rendszert, amivel azután módjában áll becsatlakozni észrevétlen hallgatóként bármilyen csevegésbe.

Szociális vonzatai

A személyi és szociális vonzatai még ennél is komolyabbak. A csevegő szoftvereket frissíteni kellene a fantom protokoll támogatására. Ez vajon mindenkit érinteni fog-e, függetlenül a földrajzi elhelyezkedésétől? Kanadai felhasználót érinteni fog-e, ha az alkalmazást brit törvény szerint frissítik? Ez ajtót nyit bármely kormány számára, a diktatúráknak is, hogy minden erőlködés nélkül és titokban kémkedjenek a polgáraik után.

Emlékszel az Edward Snowden ügyre?

Ha egy szoftvernek két változata van – egy brit és egy a világ többi részének – hogyan fognak együttműködni? Egy a Királyságba látogató kanadai tudja-e majd használni a csevegő alkalmazást? Valószínűleg nem, hacsak nem frissít a fantom protokollal együttműködőre. A frissítés ott marad majd a telefonján hazatérte után is.

A bűnüldözésnek feltétlenül szüksége van, hogy hozzáférjen információkhoz, a biztonság és bűncselekmények feltárása érdekében és a technológia ezt nehezíti. Ám bűnüldözők információgyűjtési kapacitása nem növelhető úgy, hogy közben egyének személyiségi jogait aláássák, amit a fantom protokoll eredményez. Sokakat tesz sérülékenyebbé csak azért, hogy Britannia kémkedhessen pár ember után.