SYN-elárasztás elleni védekezés a RESPIRE algoritmus segítségével

Korn András, Dr. Fehér Gábor, Gyimesi Judit

Számos ismert webszervert bénítottak meg rosszindulatú felhasználók hosszabb-rövidebb időre egy SYN-elárasztás (SYN flood) néven ismert támadás segítségével. Ezeknek a támadásoknak a kivédésére több olyan módszert javasoltak, amely bevált és elterjedt. Cikkünkben azonban egy olyan újszerű megoldást ismertetünk, amely lehetőséget biztosít a SYN-áradatok automatikus felismerésére és szűrésére anélkül, hogy számottevő többletterhelést okozna az áldozaton. Hatékonyságát mind szimulációval, mind numerikus analízissel alátámasztjuk.

Az itt javasolt módszer nem igényli további adatgyűjtő eszközök elhelyezését. Azokat az adatokat használjuk fel a támadás felismerésére, amelyeket az áldozatnak amúgy is gyűjtenie kell ahhoz, hogy TCP szolgáltatást legyen képes nyújtani.

SYN-áradat esetén a kimenő SYNACK csomagok és a bejövő, kapcsolat-felépítést véglegesítő ACK csomagok aránya sokkal nagyobb lesz egynél. Mivel a legtöbb válasz nélkül maradó SYNACK csomagot éppen a támadó SYN-csomagjaira adott válaszként küldjük el, a támadót úgy találhatjuk meg, ha megkeressük az(oka)t a hálózato(ka)t, amely(ek)nél nagy az egy érvényes bejövő ACK csomagra eső kimenő SYNACK csomagok száma.

Ezt a problémát úgy oldjuk meg, hogy a kimenő SYN ACK és a bejövő ACK csomagok C osztályú hálózatonkénti számát nyilvántartjuk; a számlálókat egy dinamikusan bővíthető hierarchikus adatstruktúrában, egy 256-odrendű fában tároljuk, kihasználva az IP-címek hierarchikus jellegét.

Megmutatjuk, hogy a különösen nagy intenzitású támadások felismerése, a támadó azonosítása és a támadás kiszűrése rendkívül gyorsan, fél másodpercnél is rövidebb idő alatt megtehető. Bebizonyítjuk továbbá, hogy az algoritmus reakcióideje a támadás intenzitásának növelésével csökken.