TEMATIKA:

DHA VÉDELMI RENDSZER EREDMÉNYEINEK STATISZTIKAI VIZSGÁLATA

Szabó Géza, szabog@crysys.hu
Bencsáth Boldizsár, boldi@crysys.hu
Budapesti Műszaki Egyetem Híradástechnikai Tanszék

Az elektronikus levelező-szerverek által karbantartott levélcímek megszerzésének egyik lehetséges módja a címkinyerő támadás (*Directory Harvest Attack*).
A DHA problémája az SMTP protokollban gyökeredzik: a levelező szerverek, ha megfelelő e-mail címre kapták a levelet, úgy nem adnak visszajelzést, elfogadják azt. Amennyiben egy érkező levél nem az általuk karbantartott felhasználók címére lett küldve, úgy vagy azonnali, vagy későbbi visszajelzést adhatnak a levelező-szerverek arra nézve, hogy a kapott levélben szereplő felhasználó postafiókja nem létezik a nyilvántartásukban. Ez a folyamat információval szolgál a levelező-szerver által karbantartott e-mail címekről. A támadók ezt az információt használják ki, nagy számú levelet küldve az adott e-mail szervernek. Azokról a címekről, amelyekről nem érkezik válasz, azaz a szerver negatív visszajelzés nélkül elfogadja a levelet, nyilvántartást vesznek fel. Ezek a címek minden valószínűség szerint érvényes felhasználói azonosítókhoz tartoznak, így érdemes lehet rájuk a későbbiekben kéretlen leveleket küldeni.

Előadásunkban spamvédelmi módszerek területén végzett kutatásainkat és fejlesztési terveinket, eredményeinket kívánjuk vázolni. A tervezett védekezési módszerek komponens alapú fejlesztések, egymással szorosan összefüggő módszerek, amelyek egymás szoftverelemeit is jelentős mértékben felhasználják.
Tavalyi előadásunk alkalmával bemutattunk egy lehetséges megvalósítás tervet. Ezt a munkát folytatva implementáltuk a rendszert és működtettük huzamos ideig adatokat gyűjtve a támadókról.
Elemezni kívánjuk a rendszerünk által összegyűjtött adatokat. Bemutatjuk, hogy milyen tipikus DHA támadók vannak, és hogy ezeket meg lehet-e különböztetni egyértelműen egymástól pusztán a támadási statisztikákból. A támadók ország szerinti megoszlását európai viszonylatban összehasonlítjuk. A magyarországi DHA körképet áttekintjük internetelérés alapján. Megvizsgáljuk, hogy a modern statisztikai módszerekkel választ kaphatunk-e arra, hogy miért is történik a DHA támadás.