Vuvuzela następca Tora?

11 grudnia 2015

Naukowcy z MIT-u ogłosili powstanie sieci służącej do bezpiecznego przesyłania wiadomości tekstowych. Twierdzą, że jest ona bardziej bezpieczna niż Tor i nawet najpotężniejsze organizacje nie są w stanie wyśledzić, jak przebiega komunikacja.

Technologia Vuvuzela wprowadza do sieci szum składający się z przypadkowych sygnałów, które ukrywają, kto z kim się komunikuje. Ten sposób zapewniania anonimowości jest znacznie bardziej skuteczny niż sposób działania Tora. W ubiegłym roku badacze z MIT-u dowiedli, że możliwe jest śledzenie użytkowników sieci cebulowej. „Tor opiera się na założeniu, że nie istnieje globalny gracz zdolny do śledzenia każdego połączenia. Obecnie to założenie nie jest już raczej prawdziwe. Tor zakłada również, że nie istnieje jedna organizacja zdolna do przejęcia kontroli nad dużą liczbą węzłów. Sądzimy, że obecnie istnieją organizacje, które mogą przejąć kontrolę nad połową węzłów Tora" – mówi profesor Nickolai Zeldovich, który stał na czele grupy rozwijającej Vuvuzelę. Sieć zwiększa stosunek szumu do sygnału do tego stopnia, że istnieje duża matematyczna gwarancja anonimowości.

W sieci Vuvuzela pozostawia się informację pod konkretnym adresem pamięci serwera. Odbiorca musi odwiedzić ten adres i odczytać wiadomość. Taka komunikacja byłaby łatwa do wyśledzenia. Vuvuzela wprowadza więc do sieci automatycznie generowane fałszywe informacje. Mimo to ktoś, kto byłby w stanie zinfiltrować sieć mógłby również domyślić się, kto z kim się komunikuje na podstawie statystyk i wzorców odwiedzin serwera przez konkretne osoby. Aby zapobiec takiej infiltracji Vuvuzela korzysta z wielu warstw szyfrowania, a informacje są przesyłane przez liczne przypadkowe węzły. Każdy z węzłów odejmuje jedną z warstw szyfrowania, prawdziwa informacje trafia tylko do serwera docelowego. Nadal jednak nie

gwarantuje to ochrony przed napastnikiem z odpowiednimi zasobami i umiejętnościami. Dlatego też Vuvuzela korzysta jeszcze z dodatkowego zabezpieczenia. Każdy z węzłów w sieci generuje dużą ilość zaszyfrowanych fałszywych informacji i wysyła je w różnych kierunkach. To, jak twierdzą twórcy sieci, powoduje, że „statystycznie jest niemal niemożliwe, by podsłuchujący był w stanie stwierdzić, czy którakolwiek z wiadomości wysłanych w tym samym okienku czasowym dotarła do tego samego punktu docelowego".

Profesor Michael Walfish z New York University przyznaje, że osiągnięcie kolegów z MIT-u jest niezwykle interesujące z punktu widzenia zachowania prywatności, zauważa jednak, że ma ono poważne ograniczenia. Największym problemem Vuvuzeli, jak podkreślają sami twórcy systemu, jest znacznie ograniczona prędkość przesyłania danych. Możliwe jest wysłanie jednej wiadomości na minutę. „To system, który nie jest jeszcze gotowy do rzeczywistego zastosowania. Jednak, jak dotąd, jest to najlepszy akademicki system zainspirowany Torem. To ekscytujące osiągnięcie, które otwiera drzwi do opracowania w niedalekiej przyszłości czegoś praktycznego" – mówi uczony.

Anonimowość w internecie jest wciąż przedmiotem sporów. Z jednej strony obywatele chcą i mają prawo zabezpieczyć swoją komunikację przed rządem, z drugiej jednak strony z technologii zapewniających anonimowość korzystają m.in. przestępcy i terroryści. Wobec kolejnych ataków, takich jak w Paryżu czy San Bernardino, pojawiają się propozycje coraz bardziej radykalnych rozwiązań. Francuski rząd chciałby np. zakazać stosowania sieci Tor.

Autorstwo: Mariusz Błoński
Na podstawie: ITPro.co.uk
Źródło: KopalniaWiedzy.pl