Użytkownik nie ma szans

Rozmowa z profesorem **Mirosławem Kutyłowskim**

Michał Koralewski: *Trudno sobie wyobrazić współczesną bankowość elektroniczną bez bezpiecznej transmisji danych poprzez protokół SSL. Ataki kleptograficzne, w miarę swojego rozwoju, mogą jednak poważnie zachwiać wiarą w bezpieczeństwo transakcji internetowych. Czy przeciętny Kowalski może się przez tymi atakami zabezpieczyć?*

Mirosław Kutyłowski: Kowalski może w bardzo znacznym stopniu ograniczyć niebezpieczeństwo. Po pierwsze, lepiej unikać serwisów, w których autoryzacja opiera się wyłącznie na haśle i numerze klienta. Te mogą zostać podsłuchane (kleptografia stanowi tu tylko jedną z metod, bardzo niebezpieczne są wirusy rejestrujące to, co wpisujemy na klawiaturze). W sytuacji, gdy do przeprowadzenia transakcji potrzebny jest kod jednorazowy podany przez token lub z listy ze zdrapkami, atak jest bardzo utrudniony – atakujący musi działać natychmiast. Po drugie, jeśli stosujemy oprogramowanie z niedostępnym kodem źródłowym, to róbmy to tylko w sytuacji, gdy do producenta posiadamy naprawdę pełne zaufanie.

M. Koralewski: *W jaki sposób można poznać, że nastąpił atak kleptograficzny, skoro nawet testy zgodności produktu z danym protokołem nie będą wykazywały żadnych podejrzanych odstępstw?*

M.Kutyłowski: Inaczej niż w przypadku pozostałych ataków, poznać jest bardzo trudno. Kod kleptograficzny nie powoduje żadnych zmian w zachowaniu systemu. Żadne dodatkowe informacje nie są wysyłane pod nieznane adresy, stosowane cookies wyglądają losowo, połączenia są nawiązywane zgodnie z protokołem... Pojedynczy użytkownik nie ma tu większych szans. Zadanie to może okazać się niezwykle trudne nawet dla profesjonalisty posiadającego odpowiednią wiedzę. Jedyna metoda, to analiza wykonywanego kodu i wyszukiwanie w nim fragmentu, który implementuje kleptograficzną zapadkę. Niestety, do ukrycia takiego kodu mogą być użyte techniki, które miały służyć do umieszczania cyfrowych odcisków palców w softwarze. Nie są to techniki niezawodne, ale mogą bardzo podnieść koszt analizy.

Fot. Bartłomiej Rożański

M. Koralewski: *W drugiej połowie maja w Warszawie odbędzie się demonstracja działającego algebraicznego ataku na szyfry blokowe. Wydarzenie to określa się jako unikalne i bardzo ważne w świecie naukowców. Jakie zagrożenia płyną z tego typu ataków?*

M. Kutyłowski: W istocie, w ostatnich latach duże postępy odnotowano w rozwijaniu metod algebraicznych łamania szyfrów symetrycznych. I wciąż wygląda na to, że nie zbliżyliśmy się do końca tej historii. *Co do zagrożeń – po prostu używając szyfry blokowe powinniśmy mieć świadomość, że być może za parę lat będzie można je złamać. Że nie należy liczyć, iż AES będzie odporny na ataki przez najbliższe 1000 lat.*

M. Koralewski: *Do jakich ataków dochodzi obecnie najczęściej?*

M. Kutyłowski: Sądzę, że do tych najprostszych, takich jak phishing. Dziś już zapewne większość użytkowników nie daje się nabrać na emaile z żądaniem podania hasła, ale… zapewne za jakiś czas doczekamy się kolejnego tricku. Z drugiej strony, obecna sytuacja może być taka jak z Enigmą w czasie II wojny światowej. Wtedy jedną z najpilniej strzeżonych tajemnic był fakt, że szyfr ten został złamany przez tajne służby aliantów.

M. Koralewski: *Podczas konferencji we Freiburgu przedstawią Państwo – tzn. Pan, Marcin Gogolewski, dr Marek Klonowski, dr Przemysław Kubiak, Anna Lauks i Filip Zagorski – metody ataków skuteczne w stosunku do prawie wszystkich produktów wykorzystywanych do wyborów drogą elektroniczną…*

M. Kutyłowski: Chodzi o ataki na protokoły, więc niezależne od konkretnych implementacji. Wykazaliśmy, że do kilku najważniejszych protokołów e-wyborów można wbudować zapadki kleptograficzne. Umożliwiają one sprawdzenie jak głosowała konkretna osoba. Taki sposób przeprowadzenia e-wyborów prowadzi do zaprzeczenia idei demokracji – wyborcę można z jednej strony zastraszyć, a z drugiej strony można skupywać głosy. Czasami atak pozwala również na zmianę oddanych głosów.

M. Koralewski: *Dziękuję za rozmowę.*