Cyberdefence 24

18.10.2017

ATAK KRACK NIE TAK POWAŻNY JAK POCZĄTKOWO SĄDZONO [KOMENTARZ EXATELA]

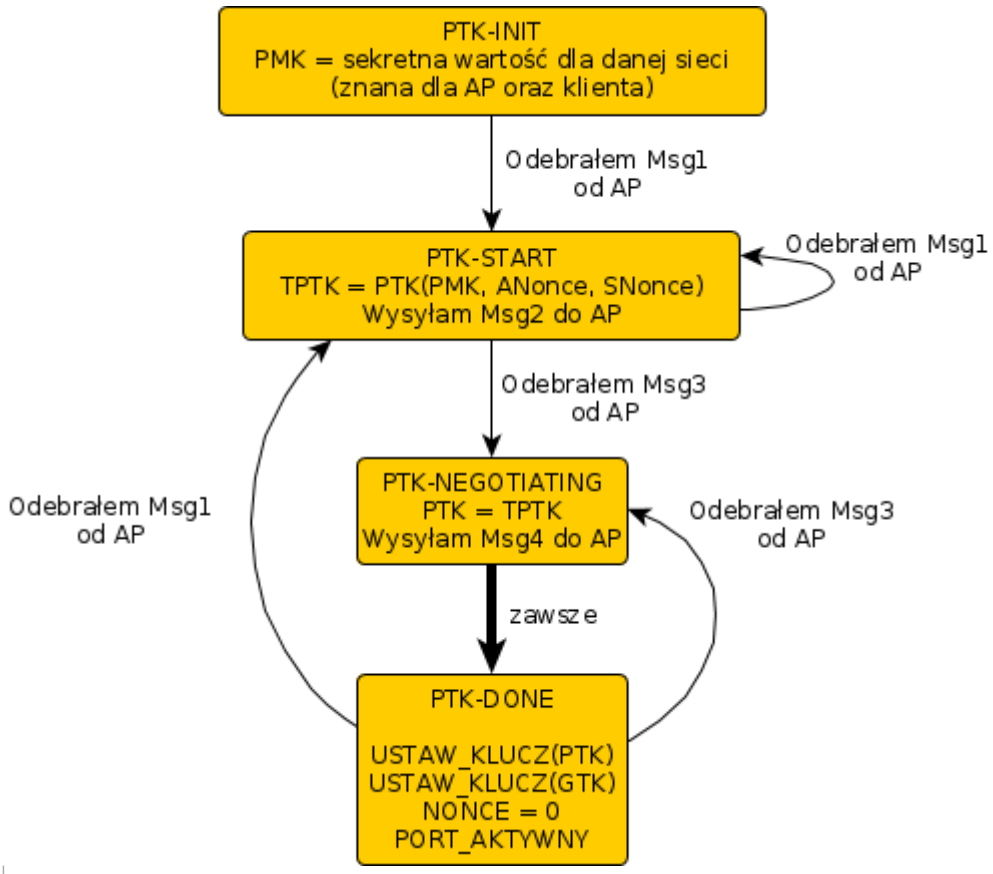
Atak KRACK polega na skłonieniu karty WiFi do przewidywalnego zaszyfrowania transmisji danych przez złamanie zasady używania tak zwanych liczb nonce. Nonce to termin używany w kryptografii do określenia takiej liczby, której używa się **tylko raz**, bo jej ponowne użycie w protokole kryptograficznym kończy się naruszeniem poufności lub integralności danych.

Jak to działa

Atak jest możliwy dzięki sprytnemu wykorzystaniu mechanizmu retransmisji pakietów podczas operacji uzgadniania wspólnych kluczy, tzw. "4-way handshake". Operacja ta przebiega pomiędzy kartą WiFi klienta (np. telefonem czy laptopem) a access-pointem (AP) i jak można się domyślić z nazwy, polega na wymianie czterech wiadomości. Pełni ona jednocześnie kilka funkcji:

- uwierzytelnia stację klienta wobec access-pointa i access-point wobec klienta, 4-way handshake powiedzie się tylko wówczas, gdy obie strony znają wspólny sekret, specyficzny dla danej sieci WiFi (tzw. PMK → Pairwise Master Key),
- ustala wartość kluczy wykorzystywanych później do szyfrowania pakietów z danymi przesyłanymi dla użytkownika (np. z zawartością oglądanych przez nas stron internetowych). Szczególnie interesujące są klucze PTK (ang. Pairwise Transient Key) oraz GTK (ang. Group Transient Key).

Dla zrozumienia przebiegu ataku konieczne jest poznanie działania operacji 4-way handshake w jej podstawowym wariancie (używanym podczas łączenia się klienta z siecią WiFi). Z perspektywy stacji klienta proces wygląda tak:



Fot. Exatel

Dla odkrytej podatności krytyczny jest pakiet numer 3 (nazwany "Msg3" na rysunku), który przesyłany jest z access-pointa do stacji klienta. Odebranie tego pakietu przez stację klienta skutkuje przejściem do stanu "PTK-NEGOTIATING" i wykonaniem dwóch operacji:

- „aktywowania” uzgodnionych kluczy (PTK i GTK) jako bieżących kluczy do szyfrowania pakietów przesyłanych łączem radiowym,
- resetu wartości nonce używanej podczas szyfrowania pakietów danych do stanu początkowego (zero)

W zwykłych okolicznościach 4-way handshake przebiega w czterech krokach z góry na dół” rysunku. Jednak komunikacja odbywa się w medium radiowym, w którym wysyłane pakiety często nie docierają do adresata, projektanci protokołu przewidzieli kilka scenariuszy retransmisji poszczególnych wiadomości. Zwróćmy uwagę, że nawet gdy 4-way handshake zostanie z sukcesem zakończony (gdy stacja klienta dojdzie do stanu "PTK-DONE"), odebranie poprawnego pakietu Msg3 niejako restartuje proces i ponownie ustawia klucze PTK i GTK, resetując również wartość nonce do stanu początkowego (zero).

Wartość nonce jest wykorzystywana do szyfrowania pakietów z danymi, a atakujący jest w stanie wytworzyć sytuację, w której stacja klienta ponownie wykorzysta taką samą wartość nonce. To poważne naruszenie bezpieczeństwa kryptografii. Atakujący, generując retransmisje wiadomości Msg3 może zostać niechcianym „pośrednikiem” komunikacji i mieć wgląd w informacje i możliwość ich podmieniania. Tego typu atak jest nazywany man-in-the-middle.

Po zapisaniu przez atakującego zaszyfrowanych pakietów z powtarzającymi się numerami nonce, jego dalsze kroki zależą od konfiguracji sieci WiFi, a konkretnie od zastosowanego wariantu protokołu szyfrowania pakietów z danymi: TKIP, CCMP lub GCMP. Wszystkie te protokoły wykorzystują szyfrowanie w trybie strumieniowym. Strumień szyfrujący (ang. keystream) jest zależny od wartości

nonce, dlatego zawsze będzie możliwe odszyfrowanie części przesyłanych pakietów. We wszystkich trzech przypadkach możliwe są też ataki typu replay, polegające na retransmisji zarejestrowanych wcześniej pakietów.

Sieć WiFi wykorzystująca protokół CCMP daje atakującemu najmniejsze możliwości. Może on deszyfrować część ruchu sieciowego oraz wykonywać ataki typu replay. Dla porównania, w sieciach WiFi wykorzystujących protokół GCMP, atak KRACK daje atakującemu pełną kontrolę nad ruchem sieciowym z możliwością odszyfrowywania oraz generowania dowolnych pakietów przesyłanych przez AP i stację klienta. Sytuacja w przypadku protokołu TKIP jest mniej więcej pośrodku. Atakujący może generować dowolne pakiety w jednym kierunku.

Kto jest zagrożony

Mechanizm 4-way handshake jest wykorzystywany we wszystkich sieciach WiFi wykorzystujących szyfrowanie WPA2 – zarówno w sieciach korzystających z zabezpieczenia hasłem, jak i rozwiązaniach „WPA-Enterprise".

W artykule [link] opisano kilka różnych scenariuszy ataku KRAK. Uwzględniają one różnice w sposobie implementacji mechanizmów 4-way handshake w różnych systemach operacyjnych, jak również wykorzystanie ataku w nietypowych sytuacjach, np. w mechanizmie szybkiego roamingu stacji klienta pomiędzy access-pointami.

Niepożądane działanie opisanych powyżej mechanizmów nie jest problemem implementacji standardu WiFi, ale wynika bezpośrednio ze specyfikacji protokołu. Na opisany atak podatne są praktycznie wszystkie urządzenia z WiFi, w tym pracujące pod kontrolą Linuksa, Androida, Windowsa, OS X-a, iOS-a, Mac OS-a, OpenBSD. Interesujące jest to, że systemy Windows oraz iOS są najmniej podatne na ataki KRACK, bo nie implementują 4-way handshake zgodnie ze standardem i nie dopuszczają retransmisji wiadomości Msg3. W ich przypadku może być zaatakowany jedynie klucz grupowy (GTK - Group Transient Key).

Wisienka na torcie w wpa_supplicant

Atak KRACK na implementację klienta wpa_supplicant w wersjach 2.4, 2.5 oraz 2.6,
jest wyjątkowo niebezpieczny, ze względu na błąd skutkujący ustawieniem klucza składającego się z samych zer po odebraniu retransmitowanej wiadomości Msg3. W wyniku tego błędu wszystkie pakiety z danymi przesyłane przez stację wysyłane są efektywnie bez żadnego szyfrowania. W tym przypadku atakujący może nie tylko podsłuchiwać transmisję, ale również aktywnie na nią wpływać tak, jakby użytkownik znajdował się w „otwartej" sieci WiFi. Powaga tej sytuacji została przedstawiona w filmie demonstracyjnym. Z powyższego powodu zainstalowanie aktualizacji dla systemów korzystających z wpa_supplicanta jest krytyczne.

Jak się chronić

Cała opisana sytuacja jest poważna, ale nie beznadziejna. Odkryta podatność w 4-way handshake może zostać poprawiona przez niewielką modyfikację implementacji, która nie wpływa na kompatybilność z niezałatanymi urządzeniami. Część producentów urządzeń WiFi (np. Mikrotik, Ubiquity czy Aruba) już udostępniło poprawki likwidujące podatność KRACK. Należy więc monitorować kanały komunikacji producentów i jak najszybciej zainstalować poprawki, które zostaną opublikowane. Należy również zwrócić uwagę na fakt, że złamanie szyfrowania samej sieci WiFi atakującemu niewiele da, gdy ruch wewnątrz tej sieci jest zabezpieczany za pomocą poprawnie wdrożonego protokołu TLS lub SMB. Innymi słowy, czas wymienić wbudowane certyfikaty w wewnętrznych usługach naszej organizacji i zadbać o ich poprawną konfigurację. Użytkownicy korzystający z

połączeń VPN również posiadają dodatkową ochronę. Opisane scenariusze ataku KRACK mają również typowe bolączki ataków na sieci bezprzewodowe, gdzie sukces atakującego w dużej mierze zależy od warunków propagacyjnych sygnału WiFi w danym miejscu i czasie.

Jeśli więc zadbaliśmy o pozostałe warstwy naszego systemu bezpieczeństwa tak, jak uczą nas kodeksy najlepszych praktyk, możemy znacząco zredukować ryzyko wprowadzane przez KRACK.

Maciej Grela – ekspert ds. cyberbezpieczeństwa, Exatel