Sieci bezprzewodowe, tworzone w oparciu o rozwiązania Meru Networks, są odporne na zagrożenia związane z niedawno wykrytą „Luką 196" w protokole szyfrowania WPA2. Pełne bezpieczeństwo Meru zawdzięcza autorskiej technologii Virtual Port.

Istnienie błędu w protokole WPA2 - używanym do ochrony informacji w sieciach Wi-Fi - ujawniła firma AirTight. Błędowi nadano nazwę „Luki 196", ze względu na numer strony dokumentacji WPA2, na której znajduje się opis wykorzystywanych w tym protokole kluczy: PTK (Pairwise Transient Key) oraz GTK (Group Temporal Key). To właśnie błędne zdefiniowanie właściwości drugiego z tych kluczy umożliwia przeprowadzenie ataku w sieci bezprzewodowej.

„Klucz PTK jest unikalny dla każdego klienta sieci WLAN i służy do zabezpieczania transmisji unicastowych. Z kolei klucz GTK jest wspólny dla wszystkich urządzeń przypisanych do konkretnego BSSID i służy do zabezpieczania danych w transmisjach broadcastowych, czyli do wielu klientów w sieci. O ile klucz PTK jest w stanie wykryć fałszowanie danych i podszywanie się pod adresy MAC, to już klucz GTK tego nie potrafi. Korzystając z tej ułomności, osoba podłączona i uwierzytelniona w ramach określonej sieci bezprzewodowej może stworzyć zainfekowany pakiet rozgłoszeniowy, na który inne urządzenia będą odpowiadały wysyłając własny adres MAC z informacjami o kluczu prywatnym. Ta wiedza umożliwia przejęcie całkowitej kontroli nad urządzeniami z zaatakowanej sieci, przechwytywanie i deszyfrowywanie ruchu, a nawet całkowite zniszczenie sieci, np. za pomocą ataków denial-of-service. Problem ten nie występuje jednak w sieciach bezprzewodowych, które zostały zbudowane w oparciu o technologię Virtual Port dostępną w rozwiązaniach Meru Networks" - mówi Łukasz Naumowicz, Technical Support Unit Manager z Konsorcjum FEN.

Odporność sieci bezprzewodowych Meru na zagrożenia związane z Luką 196 wynika z faktu, że połączenia w tych sieciach są kontrolowane przez technologię Virtual Port. Dzięki niej, każde urządzenie w sieci WLAN posiada swój unikalny identyfikator BSSID, który jest indywidualnie generowany dla klienta i kontrolowany przez oprogramowanie Meru System Director. To z kolei powoduje, że każde urządzenie posiada też swój unikalny klucz broadcastowy dla WPA2. - „W związku z tym w sieci nie może pojawić się dwóch klientów korzystających z tego samego klucza broadcast'owego i wrogi klient nie może podszywać się pod adresy MAC punktów dostępowych i rozszerzać klucz broadcastowy, tak aby uruchomić potencjalny atak" - wyjaśnia Łukasz Naumowicz.

Technologia Virtual Port to nie jedyne rozwiązanie od Meru Networks, dzięki któremu sieci WLAN stają się coraz bardziej niezawodne i bezpieczne. Meru jest również twórcą m.in. opatentowanych technologii: kontroli i zarządzania ruchem w sieci - ATC (Air Traffic Control™) oraz technologii tzw. wirtualnej komórki (Virtual Cell™). Pierwsza z nich pozwala na ścisły nadzór nad ruchem generowanym w sieci bezprzewodowej. Natomiast wirtualna komórka umożliwia wszystkim punktom dostępowym pracę na tym samym kanale, tworząc w ten sposób jednolity obszar pokryty zasięgiem sieci WLAN. Innowacyjność rozwiązań Meru została doceniona m.in. przez Gartner Group. Firma ta dwa razy z rzędu - w raporcie z 2007 i 2008 roku „Magiczny kwadrant Gartnera dla WLAN" - uznała Meru Networks za twórcę najbardziej wizjonerskich rozwiązań bezprzewodowych na świecie. W Polsce przedstawicielem Meru jest Konsorcjum FEN. Dodatkowe informacje: www.merunetworks.pl.

Konsorcjum FEN