Cyberdefence 24

23.08.2018

PENTAGON TWORZY WŁASNY KOMUNIKATOR [KOMENTARZ EXATELA]

Marcin Kobyliński Kierownik Działu SOC Monitoring i SOC Reagowanie, Departament Cyberbezpieczeństwa EXATEL

Rząd Stanów Zjednoczonych we współpracy z Amerykańską Agencją Zaawansowanych Projektów Badawczych w Obszarze Obronności (DARPA) planuje stworzyć własny komunikator. Odporny na ataki hakerskie i szyfrujący każdą wiadomość system ma kosztować 44 miliony dolarów. Czy polskie władze powinny w takim razie rozważyć stworzenie alternatywnego rozwiązania?

Celem programu Resilient Anonymous Communication for Everyone (RACE) jest opracowanie w przeciągu 4 lat nowego systemu bezpiecznej komunikacji w Internecie. Będzie on spełniał wiele wymagających kryteriów w zakresie bezpieczeństwa i ochrony informacji. Po pierwsze system ma być „niezbyt widzialny" w sieciach teleinformatycznych. Po drugie ma zapewniać poufność, integralność i dostępność komunikatów oraz po trzecie ma on chronić prywatność każdego uczestnika systemu.

Nowy komunikator ma mieć strukturę rozproszoną, tj. z podziałem systemu na aplikacje końcowe, węzły zaufane (dystrybucyjne), co strukturalnie będzie przypominać założenia dla ARPANET (protoplasty Internetu) czy też systemów opartych o blockchain. Projektowany komunikator można porównać do rozproszonego Signala. Docelową platformą ma być zarówno dowolny komputer jak i smartphone bazujący na systemie Android.

Głównym przeznaczeniem nowego komunikatora ma być przesyłanie informacji w rozległych niezaufanych, niebezpiecznych sieciach czyli np. przez pracowników Pentagonu znajdujących się na terytorium państw uznawanych za nieprzyjazne Stanom Zjednoczonym, dlatego tak ważna jest cyberodporność systemu. Ma ona zostać zapewniona przez monitorowanie aktywności komponentów systemu, weryfikację poprawności ich działania, usuwania elementów skompromitowanych oraz generowaniem nowych poprawnie działających komponentów. Jego działanie można porównać do samoregenerującego się systemu immunologicznego. Na wszystkich poziomach systemu (aplikacji końcowych, połączeń sieciowych, przesyłanych komunikatów/wiadomości) zostanie również zaimplementowana kryptografia. Duży nacisk kładzie się również na maskowanie funkcjonowania systemu (zaciemnianie komunikacji sieciowej, dodatkową niewrażliwość na statystyczne systemy detekcji ruchu sieciowego, atomizację komponentów systemu, dystrybucji systemu z węzłów w postaci małych kawałków itd.)

Ponadto ze względu na środowisko w którym program ma działać, z góry zakłada się ryzyko skompromitowania części systemu (podsłuchania wiadomości, zamiany wiadomości, próby „zatrucia" systemu i ataku od środka itd.).

Początkowo komunikator będzie wykorzystywany przez małą liczbę osób (do 10 tys) do wysyłania

maksimum 50 wiadomości dziennie, o wielkości nie przekraczającej 1 MB. Z tego powodu wysyłanie zdjęć lub filmów będzie mniej prawdopodobne. Dopuszcza się również duże opóźnienia w przesyłaniu wiadomości. Początkowo może to być kilka godzin, docelowo ma być to 1 minuta. W dalszej fazie rozwoju planuje się ujawnienie jego kodu i komercjalizację produktu.

Warto zauważyć, że Amerykanie podzielili projekt komunikatora na 4 mniejsze projekty. Każdy z nich będzie wykonywany przez oddzielną firmę, więc w automatyczny sposób wymaga się od nich interoperacyjności. Duży nacisk kładzie się też na uwzględnienie wysokiego poziomu „testowalności" projektowanego rozwiązania.

Resilient Anonymous Communication for Everyone zostanie w całości sfinansowany z budżetu Pentagonu i będzie kosztować ok. 44 milionów dolarów. Projekt ma w pełni wejść w życie za maksymalnie 4 lata, zaś prace nad nim mają się rozpocząć już w marcu 2019r.

Charakterystyka i przeznaczenie systemu

Zakładany charakter funkcjonalny systemu RACE wskazuje na potencjalnych użytkowników (np. pracowników instytucji, agend i służb państwowych), dla których istotna będzie możliwość wysyłania krótkich, ważnych informacji czy też odbieranie takich informacji.

Przy skali wymienionej w specyfikacji należy założyć, iż użytkownikami będą osoby funkcjonujące w dość niepewnym czy nawetwrogim środowisku, korzytające z przypadkowych urządzeń/komputerów/smartphone'ow. Projektowany system RACE ma wiele zalet, cechuje się też dość naukowym i dojrzałym podejściem do realizacji przedsięwzięcia.

Słabymi elementami programu pozostaną oczywiście węzły dystrybucyjne komponentów systemu, które pomimo nacisku położonego na maskowanie komunikacji będą naturalnymi „latarniami cybernetycznymi" przyciągającymi uwagę obserwatorów. Najsłabszym elementem będzie jak zawsze użytkownik; jak również zabezpieczenia komputera/urządzenia końcowego, oraz jakość wykonania (zaprogramowania) poszczególnych komponentów systemu, tj. ilość podatności bezpieczeństwa.

Czy Polska potrzebuje analogicznego rozwiązania?

Niezależny i pewny system komunikacji rozproszonej jest bardzo przydatny dla zapewnienia bezpieczeństwa informacyjnego oraz dla pracowników struktur państwowych. Tego rodzaju rozwiązanie może stanowić istotny element cybersuwerenności każdego państwa, szczególnie jeśli zostanie wzmocnione poprzez przynajmniej częściowe wykorzystanie zaufanych i pewnych elementów państwowej infrastruktury telekomunikacyjnej oraz informatycznej.

Należy też zwrócić uwagę, iż jest to złożony projekt programowy wymagający: czasu, pieniędzy, organizacji oraz wykwalifikowanych zasobów ludzkich zaalokowanych na okres kilku lat. Nie są natomiast potrzebne duże zasoby sprzętowe, czy też infrastrukturalne, co czyni takie wyzwanie realnym w warunkach krajowych.

Wcześniej należy obliczyć ilość użytkowników w warunkach polskich oraz oszacować potrzebę biznesową i rentowność realizacji projektu typu RACE. W przypadku zrealizowania projektu przez DARPA i opublikowania kodu źródłowego zgodnie z konwencją open-source, możliwe będzie szybkie zmodyfikowanie oraz zlokalizowanie systemu na potrzeby krajowe. W przypadku upublicznienia kodu takiego systemu należy się też liczyć z jego modyfikacją oraz jego zastosowaniem przez różne podmioty w niekoniecznie dobrych intencjach, oraz z koniecznością opracowania nowych środków cyberbezpieczeństwa. Nietrwałość (ulotność) informacji przekazywanych w systemach typu RACE będzie też źródłem dodatkowych wyzwań przy zabezpieczeniu cyfrowego materiału dowodowego.