# Torowanie drogi od podwyższonego zaufania do bardziej rozbudowanych aplikacji w chmurze

Andreas Herrolz, koordynator projektu TRESSCA, objaśnia wkład prac konsorcjum w budowanie zaufania między użytkownikami chmury a dostawcami usług.

Aby przetwarzanie w chmurze osiągnęło swój pełny potencjał rynkowy, kolejnym logicznym krokiem w jego ewolucji jest przejście od magazynowania danych do ich zdalnego przetwarzania. Do tego potrzeba wysokiego poziomu zaufania wśród interesariuszy, które właśnie zamierzają zbudować partnerzy projektu TRESCCA.

Mimo iż bez wątpienia chmura czyni nasze życie łatwiejszym, świat w którym można z niej korzystać bez obaw o bezpieczeństwo nadal wydaje się mało prawdopodobny. Ostatnie naruszenia bezpieczeństwa jednych z najpopularniejszych serwisów przechowywania (przypominacie sobie Celebgate?) umocniły użytkowników końcowych w przekonaniu, że dane wrażliwe należy trzymać z dala od chmury. Podczas gdy kryptografia jest skutecznym sposobem na uporanie się z problemem przechowywania w chmurze, jej zastosowanie jest niekompatybilne ze zdalnym przetwarzaniem przechowywanych danych.

To stwarza poważny problem. Zgodnie z przewidywaniami, do roku 2016 ponad jedna czwarta wszystkich aplikacji będzie dostępna w chmurze. Uciekanie się do kryptografii nie tylko spowalnia ewolucję, ale utrudnia także dostawcom usług zaufanie klientom i umożliwienie im przetwarzania danych przechowywanych na swoich serwerach – hamując w ten sposób innowacje w sektorze.

Aby uporać się z tym problemem, partnerzy TRESCCA (TRustworthy Embedded systems for Secure Cloud Computing Applications) zamierzają zaproponować i zademonstrować innowacyjne zabezpieczenia sprzętu oraz techniki wirtualizacji na potrzeby chmury. Umożliwią one interesariuszom przetwarzanie danych wrażliwych za pomocą zdalnego silnika przetwarzania bez zmiany paradygmatu, gdyż raczej uzupełnią dotychczasowe rozwiązania o nieinwazyjne dodatki niż będą je zastępować.

Andreas Herrolz, koordynator projektu TRESSCA, objaśnia wkład prac konsorcjum w budowanie długo oczekiwanego zaufania między użytkownikami chmury a dostawcami usług, otwierając drogę do całkowicie nowego obszaru usług i aplikacji.

Obywatele UE w coraz większym zakresie polegają na aplikacjach przetwarzania w chmurze. Czy mogą się czuć bezpiecznie?

W ostatnich latach zasadniczo wzrosła niezawodność i bezpieczeństwo usług w chmurze. Obecnie zapewniają wysoki poziom komfortu i wygodę. Są szczególnie użyteczne w kontekście aplikacji mobilnych i cross-device (na różne urządzenia). Dostawcy usług w chmurze wyciągnęli wnioski z wcześniejszych błędów i na ogół poprawili poziom ochrony danych oraz bezpieczeństwo świadczonych usług. Jednak nadal przechowywanie jakichkolwiek danych prywatnych i wrażliwych w chmurze wiąże się z poważnym ryzykiem. Wydarzenia takie jak rewelacje Snowdena czy niedawne ataki hakerskie na popularne serwisy w chmurze pokazują, że nawet jeżeli dostawcy usług zapewniają użytkowników o wysokim poziomie bezpieczeństwa, użytkownicy końcowi nie mogą im w pełni zaufać.

Czy zgodziłby się pan ze stwierdzeniem, że rozwój rynku chmury jest obecnie wstrzymywany przez brak zaufania między dostawcami a użytkownikami?

Zdecydowanie tak. Chmura ma ogromny potencjał, aby istotnie zmienić sposób, w jaki korzystamy z komputerów i urządzeń mobilnych. Stanowi również podstawę przyszłych koncepcji, takich jak inteligentne miasta czy Internet rzeczy. Jednakże tak długo jak nie będziemy w stanie zagwarantować poziomu bezpieczeństwa oraz ochrony danych przechowywanych i przetwarzanych na zdalnych serwerach i go sprawdzać, tego typu aplikacje nie mogą być realizowane bez ustępstw.

Jakie rodzaje technik wykorzystuje TRESCCA, aby stworzyć bezpieczniejszą i bardziej godną zaufania chmurę?

Partnerzy TRESCCA opracowują komponenty sprzętu i oprogramowania, które przyczynią się do stworzenia bezpiecznego i zabezpieczonego środowiska na potrzeby wszelkiego typu przetwarzania. Jeżeli chodzi o sprzęt, to w ramach TRESCCA powstają zabezpieczenia zintegrowane z tak zwanymi systemami SoC. Tego typu układy scalone są już powszechnie wykorzystywane w komputerach,

smartfonach, tabletach i set-top boksach. Zabezpieczenia TRESCCA nazywane modułami zabezpieczeń sprzętowych (ang. Hardware Security Modules, HSM) chronią komunikację wewnątrz i na zewnątrz układu scalonego; na przykład wszelka próba zmodyfikowania lub odczytu danych przechowywanych w pamięci RAM komputera zostanie wykryta i udaremniona. Ponadto TRESCCA tworzy bezpieczne środowisko uruchamiania oprogramowania, wykorzystując technologię wirtualizacji, aby izolować aplikacje w małych, lekkich maszynach wirtualnych. Te wirtualne maszyny mogą być także używane do bezpiecznego przenoszenia zaufanych aplikacji między urządzeniami. Połączenie technologii HW z SW zapewnia poziom bezpieczeństwa, który może być zdalnie sprawdzany przez dostawców usług i użytkowników.
Na potrzeby demonstracji TRESCCA integruje te technologie z połączonymi z chmurą urządzeniami klientów, takimi jak inteligentne liczniki czy set-top boksy. Dzięki zapewnieniu zaufanych i sprawdzalnych środowisk uruchamiania, niektóre części aplikacji i odpowiadających im danych nie muszą być przenoszone do chmury, tylko mogą być uruchamiane lokalnie. W przyszłości ta sama technologia może być także zintegrowana z serwerami chmury, umożliwiając użytkownikom końcowym zdalną ocenę i kontrolę bezpieczeństwa serwerów przed przeniesieniem swoich danych do chmury.

Twierdzi pan, że wasz system umożliwi nowe usługi i aplikacje w chmurze. Czy może pan to wyjaśnić?

Obecnie wszelkie dane wrażliwe muszą być szyfrowane po stronie klienta zanim zostaną zapisane w chmurze, aby zapewnić ich bezpieczeństwo. Jednak to wyklucza jakiekolwiek sensowne przetwarzanie danych w chmurze. Z drugiej strony, jeżeli urządzenia użytkownika końcowego, takie jak komputer osobisty czy smartfon, nie są zaufane, to wszelkiego rodzaju przetwarzanie lokalne wykonane na tych urządzeniach nie będzie traktowane jako zaufane przez dostawców usług. W ten sposób dochodzimy do impasu w kontekście jakiejkolwiek aplikacji w chmurze, która wymaga dostępu dostawców usług do danych prywatnych i ich przetwarzania, kiedy te dane same w sobie są nazbyt wrażliwe, aby mogły być przechowywane w chmurze. Dzięki TRESCCA takie aplikacje są możliwe z zaufanymi urządzeniami użytkowników końcowych, które lokalnie przetwarzają dane wrażliwe. Wówczas do dostawcy usług przesyłane są jedynie wyniki. Zasadniczo to może skutkować zmianą paradygmatu projektowania usług w chmurze, ograniczyć monopol dostawców na dane i doprowadzić do bardziej zdecentralizowanych architektur.

Rozwiązania TRESSCA będą udostępniane nieodpłatnie. Dlaczego się na do zdecydowaliście?

Jak dotąd większość istniejących rozwiązań w zakresie zabezpieczeń sprzętowych jest prawnie zastrzeżona i dostępna na licencji albo w ogóle. Naszym zdaniem to ogranicza ich przyjmowanie się, a rozwiązania z zakresu zabezpieczeń tylko wtedy

zostaną zaakceptowane i wdrożone na szeroką skalę, kiedy każdy będzie mógł je wykorzystywać, oceniać i integrować z produktami bez żadnych przeszkód. Chcielibyśmy także nawiązać współpracę z innymi przedsiębiorcami i naukowcami, którzy wprowadzą dalsze udoskonalenia do naszych rozwiązań. Naszym zdaniem nieodpłatny model dostępu wspiera tę wizję. Niemniej partnerzy TRESCCA nadal dysponują kilkoma opcjami komercyjnego wykorzystania swojego dorobku; na przykład opracowując produkty dla użytkowników końcowych na bazie technologii TRESCCA czy też oferując usługi rozwojowe innym przedsiębiorstwom.

Kiedy spodziewacie się, że technologia trafi na rynek?

Jeżeli chodzi o rozwiązania sprzętowe, może to potrwać jeszcze kilka lat, gdyż opracowanie nowego SoC jest bardzo kosztowne i czasochłonne, zwłaszcza przy pierwszej integracji nowych komponentów. Jednak rozwiązania programistyczne TRESCCA nie są uzależnione od tych komponentów i mogą być już teraz wykorzystywane z istniejącym sprzętem. A zatem mogą pojawić się na rynku znacznie szybciej, bo w ciągu roku do dwóch lat.

Prace nad projektem są bliskie ukończenia. Jaki jest do tej pory odzew branży?

Tak naprawdę zainteresowanie nieodpłatnymi i otwartymi rozwiązaniami w zakresie zabezpieczeń sprzętowych jest bardzo duże. Są to przedsiębiorstwa z branży półprzewodników, producenci urządzeń oraz dostawcy rozwiązań w chmurze. Zważywszy, że aplikacje w chmurze obejmują swoim zasięgiem aplikacje mobilne i przemysłowe, dysponowanie niezawodnymi rozwiązaniami w zakresie bezpieczeństwa nabiera zasadniczego znaczenia, a nawet staje się niezbędne dla osiągnięcia sukcesu komercyjnego. Rozwiązania oferowane przez TRESCCA i model otwartego dostępu są niezwykle atrakcyjne dla przedsiębiorstw. Jednak nadal możemy, jak sądzę, udoskonalić sposób, w jaki objaśniamy, co tak naprawdę oferuje TRESCCA i jak można to wykorzystać do stworzenia bezpiecznych aplikacji HW/SW. Ostatecznie system TRESCCA jest jedynie częścią rozwiązania i jak w przypadku wszystkich koncepcji zabezpieczeń musi zostać powiązany z innymi i odpowiednio wykorzystany, aby osiągnąć swoją pełną skuteczność.

Więcej informacji:

TRESCCA
http://www.trescca.eu/

## Kraje

Niemcy

## Powiązane projekty

ARCHIVED

## TRustworthy Embedded systems for Secure Cloud Computing Applications

TRESCCA

22 Kwietnia 2017

PROJEKT

## Ten artykuł pojawia się w...

MAGAZYN RESEARCH*EU

**Nauka w parze z bezpieczeństwem**

## Powiązane artykuły

WIADOMOŚCI

### Zestaw narzędzi oprowadzających programistów online po chmurze

20 Listopada 2015

**Ostatnia aktualizacja:** 13 Lipca 2015