Proaktywne podejście do długofalowego cyberbezpieczeństwa

W odpowiedzi na ewoluujące zagrożenia cyberbezpieczeństwa partnerzy finansowanych z funduszy unijnych projektów SHARCS i PQCRYPTO tworzą paradygmaty bezpieczeństwa, architektury i oprogramowanie, które będą w stanie zapewnić naszym systemom ICT bezpieczeństwo i wiarygodność.

BEZPIECZEŃSTWO

W dzisiejszym połączonym świecie coraz więcej naszych codziennych czynności uzależnionych jest od cyberbezpieczeństwa. Czy będzie to bankowość internetowa, zakupy przez Internet, telemedycyna, komunikacja mobilna, przetwarzania w chmurze, czy Internet rzeczy – ludzie udostępniają online coraz więcej wrażliwych informacji i danych osobowych.

Przy stale ewoluującym zagrożeniu atakiem hakerskim, proaktywne podejście sektorów publicznych i prywatnych do cyberbezpieczeństwa staje się nieodzowne. Aby pomóc w tej kwestii, partnerzy dwóch finansowanych z funduszy unijnych projektów, SHARCS i PQCRYPTO, pracują nad nowymi paradygmatami bezpieczeństwa, architekturami i oprogramowaniem, po to by nasze systemy ICT mogły być bezpieczne i wiarygodne.

Zapotrzebowanie na znowelizowane metody szyfrowania

Dzisiaj większość naszych danych online chroniona jest albo za pomocą algorytmów klucza publicznego (RSA), logarytmów dyskretnych w ciałach skończonych albo krzywych eliptycznych. W praktyce systemy te zwykle zapewniają wystarczające zróżnicowanie, aby komunikacja online mogła być bezpieczna. Jednak wraz z wchodzeniem do użytku dużych komputerów kwantowych, zdolności tych systemów

staną się niewystarczające.

Na przykład takie poufne dane jak dokumentacja medyczna czy tajemnice państwowe muszą mieć zagwarantowany odpowiedni poziom bezpieczeństwa. Jeżeli jednak będą przechowywane na komputerze kwantowym, zastosowanie szyfrowania RSA czy krzywej eliptycznej nie zapewni już ochrony przed zhakowaniem. Kiedy UE wraz z rządami krajowymi inwestuje w opracowywanie komputerów kwantowych, naukowcy z projektów SHARCS i PQCRYPTO ostrzegają, że społeczeństwo już teraz musi przygotowywać się na konsekwencje nadejścia ery komputerów kwantowych w kontekście cyberbezpieczeństwa.

Flip Feng Shui ujawnia słabe punkty

Aby pokazać poziom zagrożenia w szerszym kontekście, współpracujący w ramach projektu eksperci-hakerzy wykorzystali nową, nie-programową i opartą na wadach technikę ataku w celu zmiany pamięci wirtualnych maszyn w chmurze. Technika zwana Flip Feng Shui (FFS) pozwala atakującemu wynająć wirtualną maszynę na tym samym hoście, z którego korzysta ofiara, aby rozpracować klucze do tej wirtualnej maszyny lub zainstalować niezauważalnie złośliwe oprogramowanie. Za pomocą takiego ataku haker nie tylko uzyskuje dostęp do danych i może je przekazać dalej, ale jest także w stanie zmieniać je za pomocą krótkotrwałych zakłóceń sprzętowych. W wyniku takiego działania serwer może otrzymać polecenie instalowania złośliwego i niechcianego oprogramowania oraz pozwalać na logowanie się nieuprawnionym użytkownikom.

Podczas jednego ataku FFS naukowcy zyskali dostęp do maszyn wirtualnych hosta, osłabiając klucze publiczne OpenSSH za pomocą tylko jednego bitu. Podczas innego ataku dostosowano ustawienia aplikacji zarządzającej oprogramowaniem poprzez wprowadzanie niewielkich zmian w adresach URL, z których pobierane jest oprogramowanie. W ten sposób serwer instalował złośliwe oprogramowanie, które było przedstawiane jako aktualizacja.

Ograniczanie przyszłych zagrożeń już dzisiaj

Nie ma wątpliwości co do tego, że zapewnienie bezpieczeństwa naszych danych online wymaga większych nakładów pracy. Tylko w ramach tego jednego testu naukowcy obalili powszechne przekonanie, że zmiany bitów sprzętowych mają ograniczone zastosowanie w praktyce. Uzbrojeni w podstawowe narzędzia FFS naukowcy byli w stanie przeprowadzić druzgocący atak end-to-end, nawet przy zupełnym braku słabych punktów oprogramowania.

Aby móc ograniczyć zagrożenia takie jak FFS i inne, stale potrzebne są coraz to nowe metody testowania i certyfikowania sprzętu oraz dostosowywania potrzeb programistycznych. Z tych względów uczestnicy przedsięwzięcia SHARCS

projektują, budują i demonstrują aplikacje tworzone z myślą o bezpieczeństwie oraz usługi zapewniające użytkownikom bezpieczeństwo od końca do końca. Równolegle partnerzy projektu PQCRYPTO pracują nad systemami kryptograficznymi, które są bezpieczne nie tylko jak na dzisiejsze potrzeby, ale także w kontekście długofalowych ataków, na jakie narażone będą komputery kwantowe. Razem projekty te stworzą portfolio bezpiecznych systemów, które odpowiedzą na ewoluujące zapotrzebowanie na cyberbezpieczeństwo urządzeń mobilnych, przetwarzania w chmurze i Internetu rzeczy.

Więcej informacji:
witryna projektu SHARCS
witryna projektu PQCRYPTO

Kraje

Grecja, Niderlandy

Powiązane projekty

HORIZON 2020

PROJEKT

Post-quantum cryptography for long-term security

PQCRYPTO

7 Września 2023

HORIZON 2020

PROJEKT

Secure Hardware-Software Architectures for Robust Computing Systems

SHARCS

5 Września 2023

Ten artykuł pojawia się w...

MAGAZYN RESEARCH*EU

Zastosowania Galileo: co przed nami

Powiązane artykuły

POSTĘPY NAUKOWE

Czy można zapobiec cyberatakom komputerów kwantowych? Unijna inicjatywa pokazuje, jak tego dokonać

26 Marca 2020

NOWE PRODUKTY I TECHNOLOGIE

Nowe narzędzia i metody ochrony infrastruktury krytycznej w Europie

19 Maja 2016

Wyznaczanie trendów w nauce: Debata nad szyfrowaniem

22 Stycznia 2015

Ostatnia aktualizacja: 6 Września 2016

Permalink: https://cordis.europa.eu/article/id/120147-a-proactive-approach-to-ensuring-longterm-cybersecurity/pl