HTTPA ma pomóc chronić dane

17 czerwca 2014

Badacze z Decentralized Information Group z MIT-u proponują, by dane użytkowników internetu chronić za pomocą większej przejrzystości. Dotychczasowe próby ich ochrony, polegające na bezpiecznym przechowywaniu i szyfrowanym przesyłaniu, nie zdają bowiem egzaminu.

Naukowcy opracowali protokół „HTTP with Accountability" – HTTPA – który automatycznie monitoruje dane użytkownika i pozwala mu sprawdzić, w jaki sposób są one wykorzystywane.

Szczegóły protokołu poznamy w lipcu, kiedy to Oshani Senevirante, magistrantka z MIT-u, oraz Lalana Kagal, główna badaczka z Computer Science and Artificial Intelligence Laboratory (CSAIL) z tej samej uczelni, zaprezentują wyniki swoich prac podczas Conference on Privacy, Security and Trust organizowanej przez Instytut Inżynierów Elektryków i Elektroników (IEEE).

Dzięki HTTPA każdy fragment danych osobowych uzyska własne URI (Uniform Resource Identifier). Za każdym razem, gdy serwer będzie wysyłał tego typu dane wraz z nimi wyśle opis zastrzeżeń dotyczących ich użycia. Wykorzystanie HTTPA będzie dobrowolne, jednak twórcy nowego protokołu wierzą, że szybko stanie się on de facto standardem. Internauci powierzający swoje dane jakiejś aplikacji chętniej zdradzą je wówczas, gdy aplikacja będzie korzystała z HTTPA.

Pani Seneviratne zapewnia, że już teraz można by wdrażać nowy protokół. „Łatwo jest przygotować już istniejącą witrynę pod kątem HTTPA. W odpowiedzi na każde zapytanie HTTP serwer powinien stwierdzać: „OK, oto zastrzeżenia dotyczące użycia tych danych" oraz zapisywać transakcję w sieci specjalnych serwerów." Przykładem użycia HTTPA mógłby być przypadek, gdy lekarz chce uzyskać dostęp do danych pacjenta stworzonych

przez lekarza podstawowej opieki zdrowotnej i uzupełnić informacje o stanie zdrowia. Wówczas otrzymałby takie dane z odpowiednimi zastrzeżeniami, a gdy uzupełni dane HTTPA oznaczy je jako informacje pochodzące od innych danych i automatycznie opatrzy je takimi samymi warunkami użycia.

HTTPA wykorzystuje rozproszone tablice mieszające do przesyłania logów transakcji pomiędzy serwerami. Pojawia się tutaj redundancja danych, dzięki czemu w przypadku awarii któregoś z serwerów dane są nadal dostępne. Poza tym pozwala to na stwierdzenie, czy w którymś miejscu nie doszło do manipulacji danymi. Łatwo będzie wychwycić serwer, w którym przechowywane dane będą niezgodne z danymi z innych serwerów.

Autor: Mariusz Błoński
Na podstawie: MIT
Źródło: Kopalnia Wiedzy