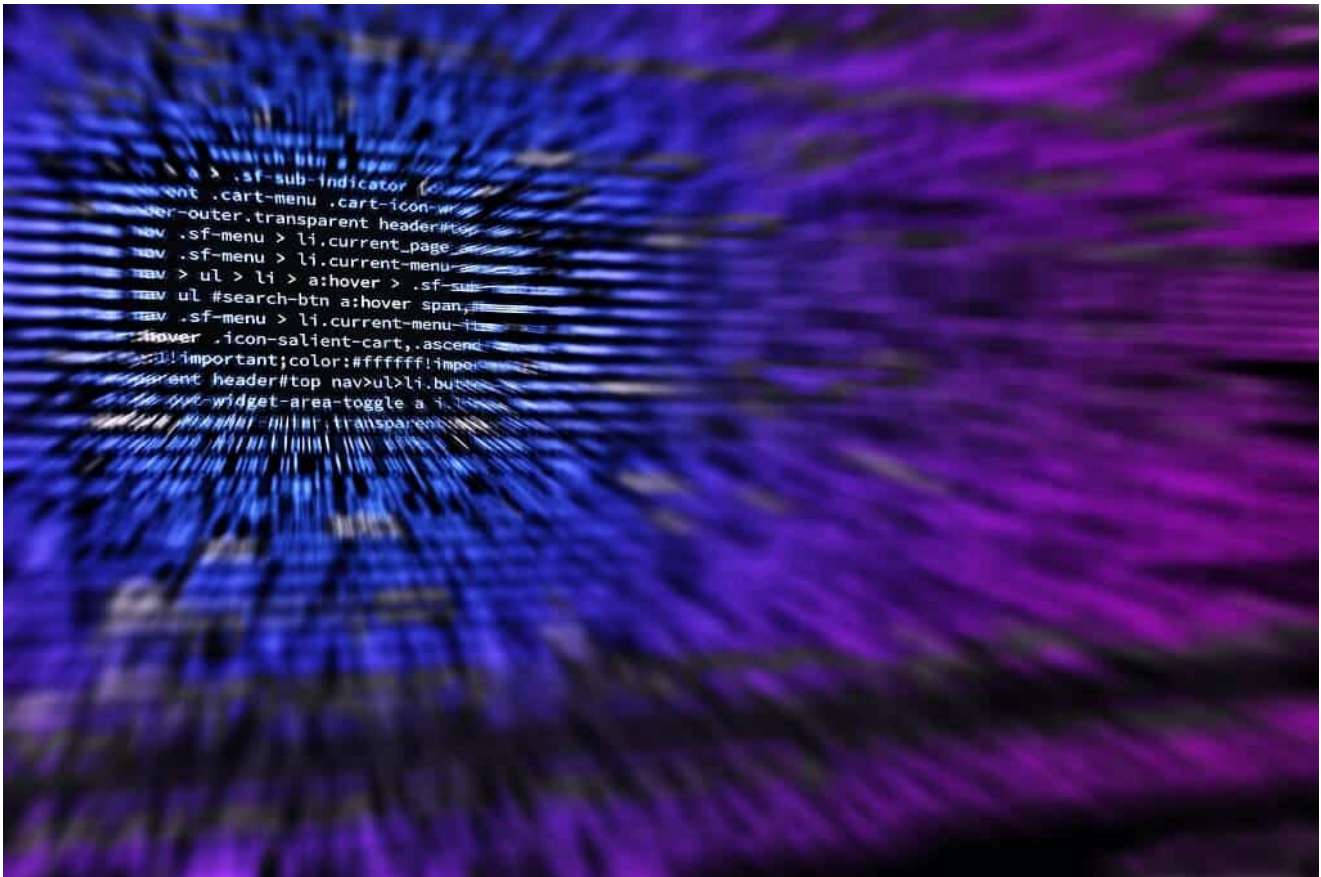


PRESSEMEDDELELSE

PRESSEMEDDELELSE: Ny løsning åbner op for sikker brug af skyen

Pressemeddelelse · Rådgivning og teknik



Alexandra Instituttet har udviklet en distribueret kryptologiløsning, der åbner op for sikker brug af cloud-løsninger. Løsningen bliver taget i brug af Alphawallet i Singapore, der har udviklet en blockchain-pung.

Single sign-on, hvor man eksempelvis logger ind og verificerer via Google eller Facebook, vinder i stigende grad frem. Metoden gør det nemmere og hurtigere at logge ind. Fordelen er, at brugerne ikke skal huske kodeord til alle de tjenester, som de bruger.

Men det åbner også op for misbrug, da en hacker nu kun skal fremskaffe et enkelt kodeord for at kunne bryde ind i alle konti hos en bruger. Eller endnu værre, hvis en hacker får

adgang til hele databasen med kodeord hos Google eller Facebook. I så fald vil hun nu kunne misbruge alle brugere på alle tjenester, hvor de har brugt single sign-on.

For at beskytte mod det har Alexandra Instituttet i samarbejde med forskere fra Schweiz, Israel og Aarhus udviklet en løsning, hvor sikkerheden er distribueret ud på flere forskellige servere. Teknologien kan anvendes i sikkerhedskritiske situationer, herunder konstruktion af digitale signaturer og til verificering af kodeord. Det lige præcis de ting, der er nødvendige for at lave single sign-on.

Data ligger på flere servere

Kernen i teknologien er, at i stedet for at du har data liggende et centralt sted, så lægger du dem ud på flere servere, som er koblet sammen kryptografisk. Det gør det mere sikkert, da en hacker nu skal bryde ind i *alle* serverne for at få en chance for at finde en brugers kodeord.

“Der skal en vis mængde servere til at verificere kodeordet. Selv hvis én af serverne bliver hacket, kan de ikke få adgang til kodeordet. Det er en meget stærk beskyttelse, hvor serverne aldrig nogensinde ser de her kodeord,” forklarer Tore Kasper Frederiksen, Senior Cryptography Engineer, der har været Alexandra Instituttets tovholder på de kryptografiske dele af løsningen.

Den nye løsning gør det også nemt at genvinde den fulde sikkerhed, hvis et par servere er blevet hacket. Normalt kræver det, at alle brugerne skifter kodeord, hvis en server bliver hacket. Det kan man undgå med distribueret sikkerhed. I de tilfælde, hvor der ikke er stjålet kodeord fra alle serverne, behøver brugerne hverken at logge ind eller at skifte kodeord.

“Hvis ikke alle dine servere er blevet hacket, er den største gevinst, at du kan køre en algoritme, som gør al den data, der er hevet ud, ubrugelig. Og det uden at det kræver, at alle brugere skal nulstille deres kodeord eller gøre noget som helst,” siger Tore Kasper Frederiksen.

I brug hos Singapore-startup

Teknologien er ved at blive taget i brug af blockchain-virksomheden [Alphawallet](#) i Singapore, som har udviklet en blockchain-pung, hvor de har bygget deres løsning oven på den distribuerede kryptologi.

“De bruger den distribuerede verifikation af kodeord samt en anden kryptografisk teknik, så deres brugere kan tage backup af deres blockchain-nøgle, som normalt ligger på telefonen. Det betyder, at de kan få rekonstrueret deres nøgle, hvis de smadrer deres telefon og stadig kender deres kodeord. Konstruktionen gør, at ingen af serverne enkeltvis kan se nøglen. Hvis man skal have fat i nøglen, kræver det, at alle serverne bliver hacket,” forklarer han.

Åbner op for sikker brug af skyen

Med distribueret sikkerhed giver det også mening at kigge på standard cloud-løsninger. Det betyder, at du ikke behøver stole på cloud-udbyderen.

“Normalt når du sender dine data op i skyen, så skal du stole på, at udbyderen gemmer dine data, så man ikke kan se dem. Men det har gang på gang vist sig ikke at være tilfældet. Det behøver du ikke her, fordi du skal bruge flere dele, hvis du har dine data distribueret hos flere udbydere. Det kræver, at de alle sammen bliver hacket eller arbejder sammen for at hive dine data ud,” forklarer han.

Den nye teknologi skulle have været præsenteret i april på [IEEE](#), der er en af verdens største sikkerhedskonferencer, men på grund af Coronakrisen er konferencen udskudt til september.

Teknologien er udviklet som en del af Olympus, der er et 3-årigt EU-projekt, som har til formål at udvikle sikrere single sign-on- og identifikations-protokoller. Det er et samarbejde mellem University of Murcia og IBM Research i Schweiz samt virksomhederne Logalty i Spanien, Scytales i Sverige og Multicert i Portugal.

I Olympus-projektet er planen desuden, at teknologien skal anvendes til at ophøje sikkerheden i kommende digitale kørekort samt i diverse finansielle applikationer.

Kilde / Logo / Foto: Alexandra Instituttet

Online: <https://pressemeddelelse.dk/pressemeddelelser/pressemeddelelse-ny-loesning-aabner-op-for-sikker-brug-af-skyen/>

Pressemeddelelsen er videreformidlet af Pressemeddelelse.dk. Pressemeddelelse.dk er ikke ansvarlig for indholdet. Spørgsmål til indholdet rettes til Alexandra Instituttet.