

DEN TEKNOLOGISKE UDVIKLING STILLER NYE KRAV TIL IT-SIKKERHED. TRENDS SOM PERVASIVE OG CLOUD COMPUTING GØR EN RÆKKE SIKKERHEDSMÆSSIGE PROBLEMSTILLINGER MERE AKTUELLE



Når computere overtager flere og flere funktioner i vores dagligdag, er det vigtigt, at vi kan stole på dem. Benytter man f.eks. intelligent medicinsk udstyr, som automatisk kommunikerer med sundhedssystemet, er det vigtigt, at personlige data hemmeligholdes, samtidig med at man kan stole på, at det er de rigtige data, som sendes frem og tilbage.

Alexandra Instituttets indsatsområde IT-SIKKERHED samler erhvervsliv og forskning omkring sikkerhedsproblematikker på pervasive computing-området.

Forsknings- og innovationschef Jakob Pagter

På erhvervssiden er en række softwarewarehouse og ekspertvirksomheder inden for sikkerhed med i samarbejdet. På forskningssiden samarbejder Alexandra Instituttet med den internationalt anerkendte kryptologigruppe på Datalogisk Institut, Aarhus Universitet.

Indsatsområdet samarbejder med forskere på DTU og Datalogisk Institut, Aarhus Universitet. Indsatsområdet er organiseret som et center med en bestyrelse bestående af repræsentanter fra erhvervsliv og forskning. Bestyrelsesformand er Søren Duus Østergaard, IBM.

SKATT

– SIKRERE OG KLOGERE PRODUKTER GENNEM TRÅDLØS TEKNOLOGI

Det er nødvendigt med en målrettet indsats, der kan klarlægge både fordele og ulemper ved trådløs teknologi på en tilgængelig og forståelig måde over for danske virksomheder. Mange af fordelene er indlysende, men der er samtidig mange udfordringer ved at afskaffe kablerne.

Blandt ulemperne er, at der kan opstå problemer med it-sikkerheden: er kommunikationen pålidelig nok, kan kun de rette snakke med enheden, eller kan kommunikationen aflyttes? SKATT-projektet studerer forskellige anvendelser af trådløs teknologi, f.eks. til styring af pumper, produktionsstyring i grisestalde og overvågning af vandmålere. Der udvikles prototyper for anvendelserne og der opbygges en generel viden, som formidles bredt via bl.a. Ingeniørhøjskolen i Århus og via



Alexandra Instituttets kursusudbud. Grundfos og Skov A/S deltager også i projektet, der er finansieret af midler fra IKT-korridoren under Rådet for Teknologi og Innovation.

Projektet har givet et stort konkret udbytte for de deltagende virksomheder, og Skov A/S er ved at integrere nogle af resultaterne fra SKATT-projektet i sine produkter.



SIKKERT, NEMT, MOBILT

– BRUGERVENLIG IT-SIKKERHED

It-sikkerhed skal være brugervenlig og mobil. Det er målet med Alexandra Instituttets forskningsprojekt ITSCI – IT Security for Citizens. Projektet udvikler bl.a. en mobil sikkerhedsløsning til netbank. Prototypen lægger den ene del af de vigtige, personlige oplysninger på mobiltelefonen og den anden på en central server, sådan at alle data ikke går tabt, hvis telefonen bliver stjålet eller

hacket. Den øgede sikkerhed består i, at man som bruger selv kontrollerer den ene side af processen med sin mobiltelefon, som på den måde fungerer som en mobil 'nøgle'. Kommunikationen mellem mobiltelefonen og den centrale server foregår via en bluetooth-forbindelse til en stationær computer. Ud over Alexandra Instituttet er partnerne i projektet Datalogisk Institut, Aarhus

Universitet, DanID, Cryptomathic, Giritech og Danske Bank. Projektet er finansieret af Det Strategiske Forskningsråds pulje 'Borgernes it-sikkerhed'.

SIKRE AUKTIONER

– AT DELE EN HEMMELIGHED MED ANDRE UDEN AT RØBE DEN

Man kan dele en hemmelighed med andre uden at røbe den. Og man kan oven i købet regne på disse hemmeligheder, så at sige uden at kigge på dem.

Teknologien hedder Secure Multiparty Computation, og stærkt forsimplet går den ud på at fordele en beregning ud over et antal forskellige computere.

Nu har teknologien fået sin første praktiske anvendelse: et nyt auktionssystem til Kontraktbørsen for handel med sukkerkontrakter.

Ud over auktioner kan systemet bruges til databasesamkøring og benchmarking, hvor deltagerne har behov for at kombinere hemmelig viden med andre uden at skulle kompromittere deres egne hemmeligheder.

Arbejdet med sikre auktioner er forankret i forskningsprojekterne SIMAP, Secure Information Management and Processing, finansieret af Det Strategiske Forskningsråds Program Komite

for Strategiske Vækstteknologier og EU-projektet CACE, Computer Aided Cryptography Engineering.

I slutningen af 2008 er stiftet et selskab, Partisia Market Design, med henblik på at kommercialisere auktioner baseret på Secure Multiparty Computation. Se mere på www.partisia.com.

