PRESSMEDDELANDE 2018-02-05

300 miljoner till cybersäkerhet – en värdefull injektion i det digitala samhället

Stiftelsen för strategisk forskning, SSF, delar ut 300 Mkr till tio projekt i fronten för cyber- och informationssäkerhet.

Sakernas internet (IoT), som sammanbinder nätverk av små inbyggda enheter med internet, används i växande omfattning inom viktiga samhällsinfrastrukturer, som fabriker, sjukhus, transportsystem, smarta hus och elnät. Komponenterna är ofta kopplade mot globala beräkningssystem vilket möjliggör en mängd nya applikationer. Samtidigt förlitar sig dessa tekniker på öppna system- och nätverkslösningar med potentiella sårbarheter. Inte minst användargränssnitt är en ingång för attacker.

Detta beror delvis på att existerande programvara för IoT inte konstruerats med säkerhet som främsta egenskap, utan snarare för att klara av begränsade resurser som ström, minne och bandbredd. Maskininlärande algoritmer introduceras också i massiv skala; de kan vara känsliga för små men illasinnade störningar av data, men än så länge saknas metoder för att utveckla robusta maskininlärningsalgoritmer för återkopplade system.

- Vår satsning på forskning inom cybersäkerhet är mycket angelägen, säger Lars Hultman, vd på SSF. Det handlar om att ta bort sårbarheten i många uppkopplade komponenter och stora nätverk. Dataintrång och feldesignade IoT-enheter kan orsaka katastrofala skador för individer, företag, och samhälle. För att få ut så mycket som möjligt av vår alltmer uppkopplade, automatiserade och självlärande värld behövs metoder och plattformar som är säkra, pålitliga och har en inbyggd förmåga att hantera fel.

De tio projekt som nu får dela på 300 miljoner kommer att analysera säkerhetsegenskaper i programvara, utveckla plattformar med nya förbättrade metoder, som kan hantera både förväntade och oväntade fel, och checka av att säkerhetsprotokoll är korrekt implementerade. Projekten handlar även om säkerhetslösningar som är skalbara och anpassade till en öppen miljö där noder, tjänster och användare ändras över tid, analys av driftsäkerhetsegenskaper, självövervakning, självläkning och självkonfiguration.

För att undvika livshotande situationer där en hacker skaffar sig kontroll över till exempel en pacemaker eller insulinpump eller där skadlig kod kan installeras behövs effektiva säkerhetsskydd. Antalet personer med implantat ökar stadigt och projektet ” Hacka inte min kropp!” riktar speciellt in sig på dessa. De kommer

att behöva skicka mätdata och behöver då organiseras i nätverk. Forskarna i gruppen har nyligen också visat att fettlagret som finns mellan muskler och hud kan användas som en radiokanal. Projektet kommer att utveckla en säkerhetsarkitektur för implantatnätverk i kroppen och säkra metoder för dessa nätverks anslutning till Internet.
Andra projekt fokuserar på säkerhetsdrivna webbsystem, nästa generations fabrik, eller den smarta staden.

Namn, lärosäte	**Projekttitel**	**Beviljat bidrag, MSEK**
Andrei Sabelfeld, Chalmers	Säkerhetsdrivna webbsystem	30
Mads Dam, KTH	Tillförlitliga fullstack programvarusystem	34
Panagiotis Papadimitratos, KTH	Säkra och privata uppkopplingar i smarta miljöer	33
Bengt Jonsson, Uppsala universitet	aSSIsT: Säker programvara för sakernas Internet	32
Alexandre Proutiere, KTH	CLAS: Cybersäkra lärande reglersystem	33
Martin Hell, Lunds universitet	Säkra mjukvaruuppdateringar för den smarta staden	22
Christian Gehrmann, Lunds universitet	Cybersäkerhet för nästa generations fabrik	30
Alejandro Russo, Chalmers	Octopi: Säker Programmering för Sakernas Internet	31
Thiemo Voigt, Uppsala Universitet	LifeSec: Hacka inte min kropp!	27
Mikael Sjödin, Mälardalens högskola	Serendipity - Säkra och pålitliga plattformar för autonomi	28

För ytterligare information kontakta:

Forskningshandläggare Olof Lindgren, olof.lindgren@strategiska.se, tel 073-358 16 69
Kommunikationschef Eva Regårdh, eva.regardh@strategiska.se, tel 073-358 16 68