

Faktablad

MSB Forskning

Publikationsnummer MSB2525 – december 2024

Byggstenar för att stärka säkerheten i sakernas internet

Sakernas internet (IoT) är en snabbt växande teknologi som redan spelar en viktig roll i många samhällskritiska funktioner. IoT används inom områden som transporter, energiförsörjning och sjukvård, där det bidrar till effektivare och smartare lösningar. Men med dessa möjligheter följer också betydande säkerhetsutmaningar. IoT-enheter är ofta små, billiga och resursbegränsade, vilket gör dem sårbara för cyberattacker. Ett enda intrång kan påverka data, störa viktiga tjänster och sprida skador till hela nätverk.

Forskningsprojektet RIOT har arbetat för att skapa ett mer pålitligt och motståndskraftigt sakernas internet. Målet har varit att utveckla nya algoritmer och tekniska lösningar som stärker säkerheten, samtidigt som resultaten är anpassade för de praktiska begränsningar som IoT-enheter innebär. Projektet har också haft ett starkt fokus på att sprida kunskap och skapa dialog mellan forskare, industri och samhället.

Projektet RIOT har utgått från ett övergripande tankesätt som speglar IoT:s unika utmaningar:

Stärka enskilda enheter

Genom att förbättra säkerheten på enhetsnivå, exempelvis genom nya metoder för säkrare inloggning och autentisering, kan vi skydda enheter från att bli enkla måltavlor för attacker.

RIOT: Resilient Internet of Things

Projektperiod

01/2019 – 08/2024

Ansvarig forskare

Docent Magnus Almgren,
Institutionen för data- och
informationsteknik,
Chalmers tekniska högskola
magnus.almgren@chalmers.se

Professor Christian Rohner,
Institutionen för informations-
teknologi, Uppsala universitet
christian.rohner@it.uu.se

Hemsida

www.resilient-iot.se

Kontakta oss:
Tel: 0771-240 240
registrator@msb.se
www.msb.se



Myndigheten för
samhällsskydd
och beredskap

Upptäcka attacker

Även med förstärkta enheter är attacker oundvikliga. Projektet har undersökt hur IoT-enheter kan utrustas för att upptäcka och reagera på angrepp, även med begränsad processorkraft och minneskapacitet.

Skydda data och kontrollera beteende

När enheter komprometteras måste vi säkerställa att insamlad data fortfarande är pålitlig och att enskilda enheter inte kan bryta mot etablerade regler. Genom tekniker som blockkedjor och smarta kontrakt har projektet utvecklat lösningar för att spåra datakällor och verifiera att enheter följer uppförandekoder.

Metodik och samhällsnytta

Projektet har kombinerat grundläggande forskning med ett systemperspektiv som tar hänsyn till balansen mellan säkerhet och resurskrav. Exempelvis har vi analyserat hur säkerhetslösningar kan förbättras utan att överbelasta IoT-enheter med begränsad processorkraft och minne. Projektet har också använt teorier som informationsteori för att undersöka hur man på bästa sätt kombinerar säkerhetsmekanismer och samarbetar för att upptäcka angrepp.

Under projektets gång har vi strävat efter att sprida kunskap och skapa dialog om IoT-säkerhet med olika samhällsaktörer. Vi har bland annat anordnat workshops för forskare, som den tematiska serien CPSIoTSec, och deltagit i Vetenskapsfestivalen för att nå en bredare allmänhet och unga människor.