Populärvetenskaplig sammanfattning på svenska

Digitala uppkopplade enheter finns nästan överallt i samhället. År 2021 fanns det fler *uppkopplade enheter* anslutna till internet än vad det fanns människor i världen. Internet of Things (IoT) eller *sakernas internet* är ett samlingsnamn för uppkopplade *enheter* med inbyggd elektronik och ofta trådlös kommunikation. Sådana små datorer styr ett brett spektrum av saker i vårt samhälle, från hushållsmaskiner och fordon till kraftverk. En viktig sektor som blir mer och mer uppkopplad till internet är tillverkningsindustrin.

Industry 4.0 är ett koncept som förutser en framtida tillverkningsindustri som är mer flexibel än dagens. Konceptet möjliggör mindre tillverkningsserier av specialiserade produkter som effektivt kan tillverkas utan tidsödande omställning av tillverkningsmaskinerna. Denna trend inom tillverkning går mot en mer decentraliserad och lättrörlig framtid.

Många enheter som driftsätts i sådana system är så kallade *resursbegränsade enheter*. I framtiden kommer dessa uppkopplade enheter vara decentraliserade och många. Därför måste de vara billiga att tillverka, driftsätta och underhålla. Resursbegränsade enheter kan ha en eller flera av följande begränsningar: svag processor, lite minne och begränsade kommunikationsmöjligheter. Många resursbegränsade enheter drivs dessutom med batteri och behöver därför hushålla med strömförsörjningen.

Ofta blir allmänheten medveten om att ett föremål är uppkopplat först när en cyberattack stör dess funktion. Få tänkte på att kassorna på Coop egentligen är uppkopplade datorer innan utpressningsvirus gjorde dessa obrukbara. När datorer och system som styr fysiska processer såsom fabriker och energiinfrastruktur kopplas upp så introduceras nya risker för cyberangrepp. Flera uppmärksammade cyberattacker har genomförts mot industriella styrsystem och engergiinfrastruktur. STUXNET år 2012, attacken mot ett tyskt stålverk år 2014, och Triton år 2017 är bara några exempel.

Denna avhandling presenterar forskning på effektiva säkerhetsprotokoll för resursbegränsade enheter. Säkerhetsmekanismer innebär alltid effektivitetskostnader. Vi har därför undersökt prestandan för protokollen OSCORE och Group OSCORE som möjliggör säker kommunikation mellan resursbegränsade enheter.

Vår undersökning visar att protokollen är tillräckligt effektiva för användning i resursbegränsade enheter.

Vårt nästa arbete var en detaljstudie av protokollet WirelessHART. WirelessHART är ett protokoll för trådlös kommunikation i en fabriksmiljö. Vår analys visar att WirelessHART är säkert så länge ingen enhet i ett nätverk har blivit hackad. Denna analys ger användare av WirelessHART konkreta bevis för säkerheten i protokollet.

Vidare har vi undersökt konceptet *digitala tvillingar* och hur dessa kan användas för att bygga en säkerhetsarkitektur för industriella styrsystem. En digital tvilling kan ses som en digital kopia av en fysisk enhet. Vi föreslår ett sätt att konstruera en digital tvilling och att hålla den updaterad med den fysiska enheten. Vår arkitektur presenterar ett nytt sätt att designa säkra industriella styrsystem.

Vi har även undersökt säkra ägarbyten av resursbegränsade enheter. Detta är ett scenario där trådlösa resursbegränsade enheter, till exempel koldioxidmätare utplacerade i en stad, skall byta ägare. Vi har tagit fram ett protokoll som tillåter en ägare av ett sådant nätverk att överföra kontrollen till en ny ägare. Vi har bevisat säkerheten för protokollet med en teknik som kallas formell protokollverifiering och implementerat protokollet för att undersöka dess prestanda. Vårt protokoll kan möjliggöra överföringen av trådlösa nätverk av sensorer och andra uppkopplade enheter mellan operatörer.

Slutligen har vi studerat integritetskyddad datainsamling och analys för uppkopplade resursbegränsade enheter, där ett vanligt behov är central insamling av data. Data som samlas in kan avslöja information som affärshemligheter om processer i en fabrik. Vi har designat ett effektivt protokoll som tillåter krypterade mätvärden att samlas in och summeras centralt utan att individuella mätvärden avslöjas.

Avhandlingens huvudsakliga bidrag är att det är möjligt att utveckla och driftsätta säkra och effektiva protokoll för resursbegränsade enheter.