Deze ochtend vond ik een hacker in mijn koelkast

De opkomst van het internet van de dingen is niet meer te stoppen en weldra zal elk ding op aarde voorzien zijn van een eigen plek op het internet. Dit is leuk, want zo zullen we van op het werk kunnen nakijken hoeveel melk er nog in onze koelkast staat of kunnen we de verwarming van de badkamer alvast een graadje hoger zetten terwijl we nog in de file zitten op een druilerige vrijdagavond. Maar terwijl wij uitkijken naar een lekker warm bad, staat de voordeur van ons geautomatiseerd huis ook open voor anderen met minder aangename bedoelingen en een massa aan mogelijkheden om al onze online dingen aan te vallen. Zullen we ons kunnen verdedigen of is de strijd bij voorbaat al verloren?

Door Christophe Van Ginneken

Deze ochtend vond ik een hacker in mijn koelkast. Het lijkt een stuk uit een slechte science fiction film. Als we echter de evolutie van technologie van naderbij bekijken, zien we dat de realiteit misschien sneller dan verwacht de fictie zal inhalen.

Sinds het internet ervoor zorgde dat elke computer - en ondertussen ook bijna elke telefoon - ter wereld online is, voelen we reeds de hete adem van de volgende revolutie in onze nek. Opnieuw wordt alles kleiner en wil men tegen elke prijs elk ding ter wereld aansluiten op internet.

Elk ding mogen we hier eigenlijk zelfs letterlijk nemen. Onder de noemer van het *internet van de dingen* wordt al enkele jaren getracht om elk toestel in ons huis te voorzien van een aansluiting op het internet. De eerste stap was de introductie van digitale televisie. Deze *digiboxen* zijn in wezen kleine computers die verbonden zijn met de televisiedistributeur via het internet. Via interactieve programmagidsen en spelletjes verrijken ze onze televisie-ervaring met een druk op de rode knop.

De makers van televisietoestellen konden niet achterblijven en al snel zat er ook in onze televisietoestellen een netwerk-aansluiting en konden we surfen op het internet zonder ook maar van scherm te veranderen. Diezelfde televisietoestellen brengen ons vandaag tevens de reclame van een electriciteitsleverancier die ons toelaat om het energieverbruik van elk toestel in ons huis te controleren. Indien nodig kunnen we zelfs onze kwistig met energie omspringende, thuisgebleven hond via het internet de toegang tot onze elektrische apparaten ontzeggen. Zelfs als we niet thuis zijn, zijn we heer en meester over ons huis.

Het succes van deze mogelijkheden werkt duidelijk aanstekelijk en van verschillende kanten hoor je verhalen over hoe fijn het zou zijn als we ons hele leven zouden kunnen besturen via het internet. Waarom zouden we immers onze koelkast niet op het internet aansluiten en deze de mogelijkheid bieden om ons te laten weten dat we nog melk moeten halen of dat die schimmelkaas nu echt wel … aan vervanging toe is?

Een wereld vol microcontrollers en sensoren

De onderliggende technologie die dit alles mogelijk maakt, is de microcontroller. Een microcontroller is in essentie een zeer kleine computer in de vorm van één enkele chip. Zo bevat hij alles wat nodig is om er software op te plaatsen en deze uit te voeren: rekenkracht, geheugen en aansluitingspunten voor communicatie met de buitenwereld.

Microcontrollers worden in de eerste plaats ontwikkeld om andere toestellen te besturen en trachten daarom zo weinig mogelijk aanspraak te maken op de energiebron van het toestel waar ze deel van uitmaken. Een laag energieverbruik gaat echter wel gepaard met een lagere rekenkracht, maar dit is doorgaans geen probleem omdat ze ingezet worden voor een duidelijk afgelijnde taak.

Dankzij hun beperkte mogelijkheden en daardoor typische werkingscontext, zijn microcontrollers relatief goedkoop en worden ze in groten getale ingezet in diverse omgevingen. In een luxewagen zitten vandaag al snel enkele honderden microcontrollers, die elk instaan voor één van de vele snufjes die onze rit aangenamer en veiliger maken.

Microcontrollers op zich zijn echter nutteloos. Ze hebben immers invoer nodig om hun taken te kunnen vervullen. In tegenstelling tot hun grote broer in onze computer thuis, beschikken ze niet over een toetsenbord en een muis om hen te vertellen wat ze moeten doen. Daarom beschikken microcontrollers over aansluitingspunten voor externe componenten die hen toelaten om informatie uit hun omgeving op te nemen en toestellen aan te sturen.

De externe componenten die microcontrollers in staat stellen om hun omgeving waar te nemen, noemen we sensoren. Deze elektronische schakelingen kunnen omgevingseigenschappen omzetten in elektrische signalen. De microcontroller kan vervolgens op basis van deze elektrische signalen een waarde bepalen voor bijvoorbeeld de intensiteit van het licht of de vochtigheid in een kamer.

Het is deze combinatie van grote hoeveelheden sensoren en microcontrollers die de evolutie van de automobielsector vooruit stuwt en ons reeds vandaag auto's aanbiedt die autonoom kunnen parkeren of zelfs voor ons remmen wanneer we dit dreigen te laat te doen.

Draadloze sensornetwerken

De ontwikkelingen omtrent microcontrollers en sensoren zijn de laatste jaren enorm geëvolueerd. Eenzelfde evolutie kunnen we optekenen bij draadloze technologieën. Mobiel internet is een dagdagelijks gegeven geworden en we voelen ons bijna naakt als we 's morgens op weg naar het werk niet even onze status op Facebook kunnen aanpassen of het gedrag van anderen kunnen tweeten.
De combinatie van deze twee werelden heeft geleid tot de ontwikkeling van draadloze sensornetwerken. Dit zijn grote hoeveelheden microcontrollers met sensoren die dankzij draadloze technologie met elkaar kunnen communiceren en zo een netwerk creëren van zogenaamde sensorknopen.
De inzetbaarheid van deze netwerken kent vele vormen. Zo kunnen overstromingsgebieden nauwgezet opgevolgd worden of kan men het trek- en kuddegedrag van dieren optekenen. Dankzij hun kleine vormgeving en zeer lage energienoden, kunnen deze sensorknopen soms wel tot meer dan een jaar functioneren aan de hand van één enkele batterij. Dankzij hun lage kostprijs worden ze dan ook beschouwd als een wegwerpbaar goed en worden ze typisch in groten getale ingezet. Zo zal indien één knoop uitvalt, dit geen echte impact hebben op de algemene werking van het netwerk, omdat de overige knopen de taken van de uitgevallen knoop gewoon kunnen overnemen.
Het hoeft dus geen betoog dat draadloze sensornetwerken een interessante basiscomponent bieden om nog meer technologische luxe te kunnen bouwen.

De realiteit achtervolgt de fictie

We schrijven midden augustus 2013. Ergens in de Verenigde Staten van Amerika leggen twee jonge ouders hun kind te slapen onder het alziende oog van hun nieuwe draadloze, met het internet verbonden, babyfoon. Wanneer zij enige tijd later de kamer van het kind opnieuw betreden, horen ze een onbekende stem obscene woorden ten berde brengen langs deze babyfoon, tot groot jolijt van de kleine spruit.
Ondertussen wordt in Europa duchtig verder gesleuteld aan de draadloze pacemaker, een wonderbaarlijk stukje technologie dat artsen toegang geeft tot het hart van hun patiënt, waar deze zich ook bevindt. Het lijkt wel een scene uit een fictie-serie waarin een hacker zich toegang verschaft tot zo'n pacemaker en zo de drager ervan vermoordt. Pure fictie? Dick Cheney denkt het in ieder geval niet. In oktober 2013 heeft hij immers het draadloze aspect van zijn pacemaker laten verwijderen om een mogelijke terroristische aanval te vermijden.

In een luxewagen zitten vandaag al snel enkele honderden microcontrollers, die elk instaan voor één van de vele snufjes die onze rit aangenamer en veiliger maken.

Toen we in 1995 genoten van de eerste acteerprestaties van Angelina Jolie in de cultfilm Hackers, leek het kunnen besturen van verkeerslichten een prachtig staaltje science fiction. Bijna 20 jaar later zijn verkeerslichten en draadloze sensornetwerken in wetenschappelijke publicaties alvast dikke vrienden en is men klaar om onder het mom van zogenaamde slimme steden, elk van deze lichten een autonoom leven te bieden. De grote omarming door het internet van de dingen lijkt nu reeds onontkoombaar.

De hacker uit de koelkast halen

Misschien lijkt het zo dat een hacker weinig kwaad kan doen in onze koelkast. Maar wat indien we morgenvroeg plots merken dat de yoghurt die we aan onze kinderen geven een groene kleur vertoont omdat onze koelkast nagelaten heeft ons te verwittigen dat de vervaldatum verstreken was. Of dat er eigenlijk nog voldoende flessen melk waren en dat we er onderweg naar huis dus geen hadden moeten kopen, nadat we een bericht hadden ontvangen van onze koelkast dat de voorraad op was? Toevallig was er die dag tevens een superinteressante promotie van een nieuw merk van zuivelproducten dat je dan toch maar eens kon proberen. Eens deze technologie zijn intrede doet in ons dagdagelijks leven, zullen we er stilaan op vertrouwen en kan de kleinste fout grote gevolgen hebben.
Zelfs buurman Jan kan niet voorbij aan de voorbeelden en stelt zich ondertussen terecht de vraag: "Ok, en wat nu?". Als we toch willen genieten van al dat moois, maar we ook nog onze kinderen een veilig ontbijt willen aanbieden, is de beveiliging van deze draadloze sensornetwerken een evidente noodzaak, omdat de dreiging van hackers - tot letterlijk in onze koelkasten - een realiteit zal worden die impact heeft op het leven van iedereen en niet slechts voor wie mee is met de nieuwste technologische snufjes.
Onder beveiliging verstaan we meestal diens eerste doelstelling: voorkomen dat iets misgaat. Maar beveiliging gaat verder dan dat. Niet alles kan voorkomen worden. In het geval van een inbraak zal men soms genoegen moeten nemen met het "in staat zijn om de inbraak vast te stellen", om zo

Terwijl Angelina Jolie in 1995 nog kon lachen met het hacken van verkeerslichten en de bijhorende verkeersravage, lijkt deze science fiction bijna 20 jaar later een bittere realiteit.

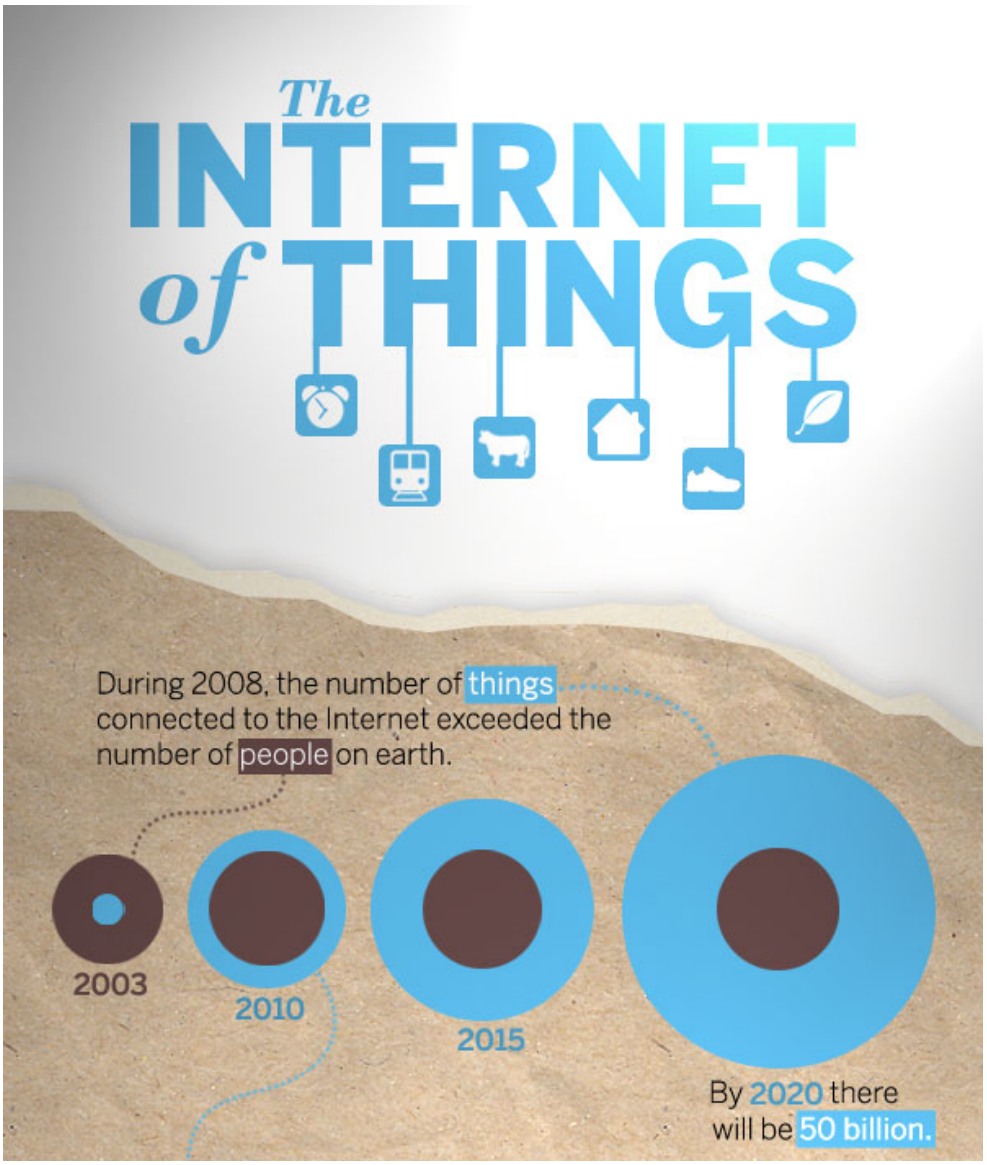
toch nog na de feiten reactieve maatregelen te kunnen nemen. In de digitale wereld is dit schering en inslag - denken we maar aan de recente onthullingen inzake de spionage in verschillende telecombedrijven. Hier worden specifieke inbraakdetectiesystemen dan ook veelvuldig ingezet om op zijn minst de inbraak vast te stellen en de schade te kunnen opmeten.

Dit is zonder twijfel ook het geval bij draadloze sensornetwerken, waar we eveneens dikwijls genoegen moeten nemen met het kunnen vaststellen van een inbraak. Maar het huwelijk van sensorknopen en inbraakdetectie blijkt al snel te stranden op basis van tegenstrijdige belangen.

Een sensorknoop is nagenoeg gedurende zijn volledige levensloop aan zijn lot overgelaten. De enige link met de buitenwereld is het draadloze netwerk dat hem toelaat te communiceren met andere knopen. Diezelfde knopen zijn tevens zijn enige communicatiekanaal met de wereld buiten het netwerk omdat communicatie over langere afstanden doorheen het netwerk van knopen vloeit.

Gedurende heel deze periode moet de knoop energie halen uit één enkele batterij en dus zeer spaarzaam omspringen met deze bron. Omdat knopen tevens in groten getale worden ingezet dient hun kostprijs zo laag mogelijk gehouden te worden. Ze zijn dan ook voorzien van maar net genoeg geheugen en verwerkingskracht om hun veelal beperkte taak uit te voeren.

Inbraakdetectie daarentegen vraagt opvolging. De meerderheid van de alarmen die door een dergelijk systeem worden gegenereerd, moeten bijna altijd nog geïnterpreteerd worden. Aangezien elke aanval verschillend is, zijn de detectiemogelijkheden ook eindeloos en wil men een inbraakdetectiesysteem typisch heel de tijd laten werken. Om optimaal te kunnen werken, dient het bij voorkeur te beschikken over enorme hoeveelheden gegevens. Deze gaan van aanvalspatronen tot modellen van normaal gedrag om anomalieën te kunnen detecteren. Tot slot is, vanuit het oogpunt van een knoop, het detecteren van inbraakpogingen een niet-functionele, bijkomende belasting.



Sinds 2008 is het aantal aangesloten elektronische toestellen reeds groter dan het aantal mensen op aarde. Tegen 2020 verwachten verschillende analisten dat dit nog zal toenemen tot 50 miljard.

Onder beveiliging verstaan we meestal diens eerste doelstelling: voorkomen dat iets misgaat. Maar beveiliging gaat verder dan dat.

Het is snel duidelijk dat de afweging tussen knoop en detectie neerkomt op het gebruik van de middelen waarover een knoop beschikt. In een ideale wereld zou een inbraakdetectiesysteem voor draadloze sensorknopen de levensduur van de batterij van de knoop niet mogen beïnvloeden, maar dat is spijtig genoeg echte science fiction.

Onderzoeksliteratuur omtrent inbraakdetectie in draadloze sensornetwerken beschrijft onnoemelijk veel manieren om specifieke aanvallen te detecteren. Een enkele uitzondering waagt zich aan een combinatie van patronen of stelt een raamwerk voor om enkele patronen te combineren. De algemene conclusie is echter unaniem: gegeven de beperkte mogelijkheden van een knoop, is het onmogelijk om een volledige dekking te bieden betreffende inbraakdetectie.

Meer zelfs, omdat een aanvaller nagenoeg te allen tijde in staat is om een knoop fysiek te benaderen, het geheugen van de knoop te raadplegen en te wijzigen, is er per definitie geen enkele mogelijkheid om elke poging tot inbraak te verijdelen zonder fysieke uitbreiding van een knoop met bijkomende, specifieke hardware. Deze zou echter de prijs van een knoop meerdere malen vermenigvuldigen en hem daarmee uit de markt prijzen.

Het beveiligen van draadloze sensornetwerken komt daarmee neer op een afweging van risico's. Hierbij is een inschatting nodig van welke aanvallen we willen onderscheppen om zoveel mogelijk barrières op te werpen om de meerderheid van de aanvallers te ontmoedigen.

In de praktijk

Indien het probleem onoverkomelijk is, rest er het draaglijker maken van de pijn. Indien we in staat zijn om de impact van de inbraakdetectie te verlichten, kan er op meer aanvallen gecontroleerd worden. Zo kan de maker van het sensornetwerk een ruimere keuze maken uit de bestaande detectiemogelijkheden, waardoor de drem-

pel voor de aanvaller toch weer een beetje hoger wordt.
De ontwikkelaar van de software van een draadloze sensorknoop kan zelf onderzoeksliteratuur raadplegen en één of meerdere van de beschreven detectiemechanismen trachten te implementeren. Hierbij zal hij typisch, voor elk van deze detectoren, een gelijkaardig blok programmacode maken dat enerzijds actief wordt bij het ontvangen van nieuwe communicatie uit het netwerk en anderzijds tussendoor de verzamelde informatie evalueert en beslissingen neemt omtrent de opgetekende situatie.
Aangezien één enkele knoop zelden een aanval of inbraak kan detecteren, is communicatie met de andere knopen een noodzakelijk kwaad. Communicatie tussen knopen is tevens de belangrijkste bron van informatie voor de knoop om zich een beeld te vormen van wat er zich rondom hem afspeelt. Nagenoeg elk detectiesysteem zal bij ontvangst van gegevens via het netwerk de inhoud ervan moeten inspecteren om zich van nieuwe informatie over zijn omgeving te vergewissen.
Anderzijds dient ook op regelmatige tijdstippen een inventaris gemaakt te worden van de verzamelde gegevens. Dit kan gaan van het controleren of er geen knopen zijn die reeds geruime tijd geen activiteit hebben vertoond, tot het berekenen van een reputatie van een knoop op basis van de verschillende gebeurtenissen in het netwerk en de informatie die andere knopen hieromtrent deelden.
Het is evident dat deze zeer gelijklopende structuur voor elk detectiemechanisme onherroepelijk kan leiden tot veel dezelfde programmacode, maar ook tot het herhaaldelijk uitvoeren van dezelfde code en talrijke berichtenuitwisselingen over het netwerk tussen de knopen, en dit voor elk van de detectoren afzonderlijk. Veelvuldige uitvoering leidt tot langere verwerkingstijden en veel communicatie leidt tot meer gebruik van het draadloze netwerk.
Voor eenvoudige detectoren lijkt dit een artificieel probleem. Elke zichzelf respecterende ontwikkelaar zal dit opmerken en zal de code zo structureren dat deze problemen weggewerkt worden. Inderdaad, voor eenvoudige systemen én indien de ontwikkelaar de volledige inbraakdetectie zelf bouwt, is dat het geval. Maar inbraakdetectie is een niet-functioneel gegeven voor de ontwikkelaar. Om inbraakdetectie economisch verantwoord te maken, zal men ook hier zoveel mogelijk gebruik willen maken van bestaande implementaties. Op dat ogenblik heeft de ontwikkelaar niet langer de luxe om de code anders te organiseren en zullen de langere uitvoertijden en het veelvuldige netwerkgebruik effectief een overmatige belasting worden voor de beperkte mogelijkheden van de sensorknoop.
Men kan echter nog verder argumenteren dat de de bijkomende verwerkingstijden bijna verwaarloosbaar zijn voor microcontrollers die amper 0.4 milli-ampère stroom verbruiken wanneer ze actief zijn - een peulschil in vergelijking met hun grote broer in onze computer die al gauw 10 volledige ampères vraagt, wat een 25000-voud is. Dit is correct, maar in dat geval mag men niet uit het oog verliezen dat een typische draadloze radio al snel 40mA verbruikt bij het verzenden en ontvangen van communicatie. Dit is een factor 100 ten opzichte van de microcontroller. Een veelgebruikte oplaadbare batterij, zoals deze in GSM toestellen, biedt gangbaar ongeveer 1700mA gedurende een uur. Een actieve draadloze radio zal de energie van deze volledige batterij op iets minder dan 2 dagen opgebruiken. Het beperken van het gebruik ervan is dus een zeer belangrijk aandachtspunt.

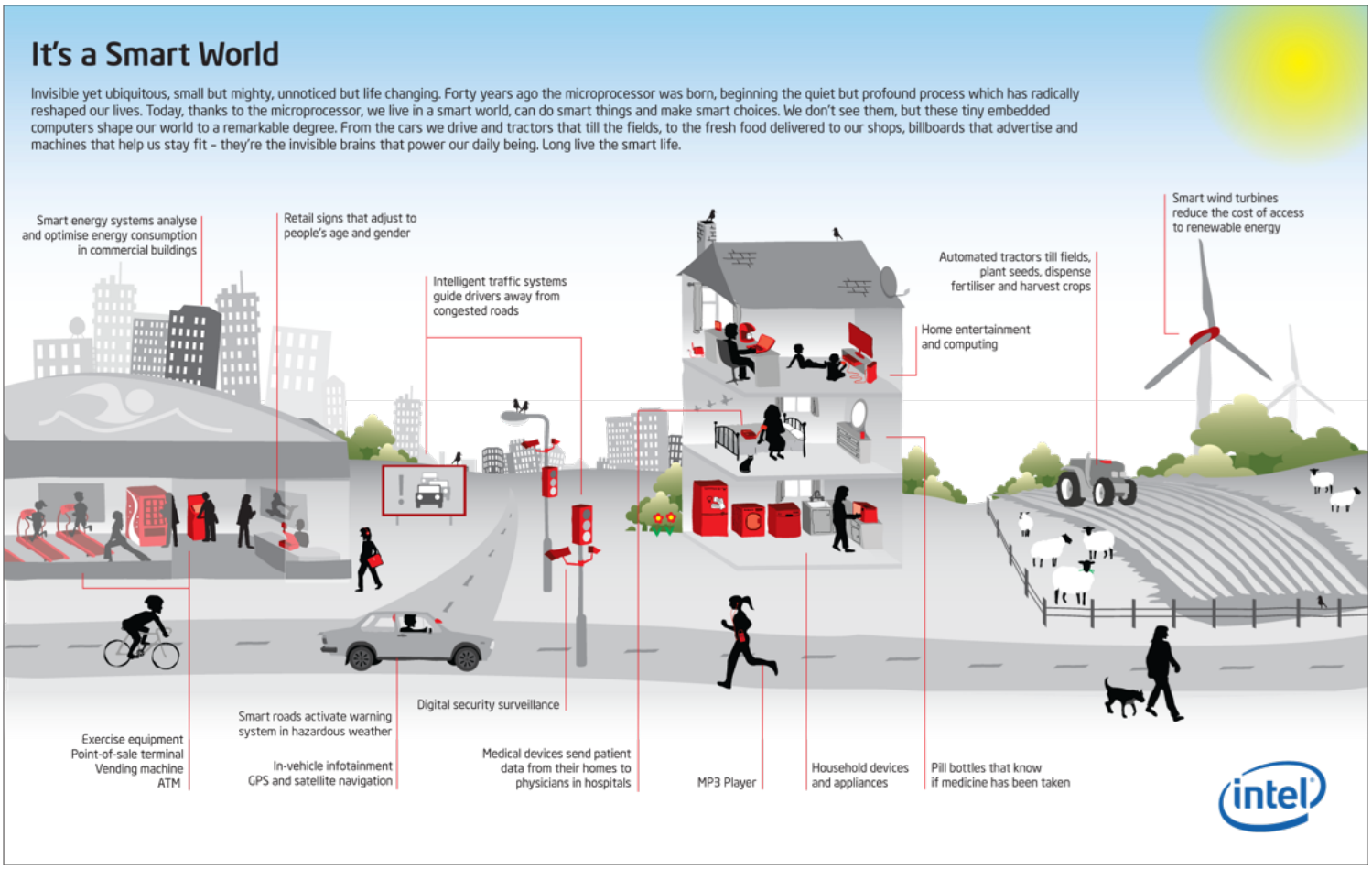
Code die code genereert

De ontwikkelaar van software voor een sensorknoop wil bij voorkeur een groot aantal bestaande detectiesystemen verzamelen en deze zo geautomatiseerd mogelijk en goed georganiseerd opnemen in zijn eigen code.
Ondanks de enorme ontwikkelingen op het vlak van taalkundige analyse, is dit echter nog steeds een nagenoeg onmogelijke taak om te automatiseren. De verschillen in stijl van programmeren van ontwikkelaars en de brede waaier aan mogelijkheden die aangewend kunnen worden, gecombineerd met de complexheid van de mechanismen die beschreven worden, maken dat het technisch niet realistisch is om bestaande programmacode van verschillende detectoren te nemen en automatisch om te zetten tot beter georganiseerde code.
Een andere aanpak bestaat erin om de beschrijving van een detector te realiseren aan de hand van een domeinspecifieke taal. Zo'n taal is opgebouwd rond een specifiek domein - in dit geval dat van inbraakdetectie - en voorziet daarvoor een typisch en vertrouwd jargon. Dit type van talen is, in tegenstelling tot normale, generieke programmeertalen, beperkt in zijn expressiviteit en bevat bv. niet de mogelijkheid om eenvoudig iteratief gedrag te beschrijven.

Een typische microcontroller (hier afgebeeld een Atmel ATMEGA328P) beschikt over een rekenkracht die ruim 200 maal lager ligt dan die van een klassieke processor. Ook qua geheugen is het verschil enorm. Met amper 2KB, of ruim 1 miljoen keer minder dan een gemiddelde desktop PC, maakt hij alvast de droom van Bill Gates uit 1981 waar. Er wordt immer gezegd dat hij toen de uitspraak deed dat 640KB meer dan genoeg was.

Deze beperking leidt er toe dat de beschrijving van een detector nog nauwelijks op meerdere manieren kan gerealiseerd worden - of alvast niet op een ongunstige manier - waardoor een geautomatiseerde verwerking sterk vereenvoudigd wordt. Hierdoor wordt één van de basisproblemen ontweken en ligt de weg open om verschillende mechanismen te combineren en optimaal te organiseren. Dit kan gebeuren door middel van specifieke codegeneratiesoftware die de beschrijving in de domeinspecifieke taal analyseert en omzet in effectieve programmacode.
Het aspect van een domeinspecifieke taal is hier het essentiële gegeven. Net door de taal toe te spitsen op één specifiek domein wordt het mogelijk om de taal zo te beperken dat de resulterende beschrijvingen geen twijfel laten over de bedoeling van de auteur en dat hij alleen maar taalelementen en constructies kan gebruiken die kunnen omgezet worden naar zo optimaal mogelijke programmacode. Codegeneratie kan al veel van de taken van programmeurs uit handen nemen, doch is vandaag nog niet in staat om algemene software te produceren op basis van een algemene functionele beschrijving.
Door aan de hand van codegeneratie de code optimaal te organiseren, wordt het

Een veelgebruikte oplaadbare batterij, zoals deze in GSM toestellen, biedt gangbaar ongeveer 1700mA gedurende een uur. Een actieve draadloze radio zal de energie van deze volledige batterij op iets minder dan 2 dagen opgebruiken.



De grote droom die veel ontwikkelingen op het gebied van draadloze sensornetwerken stuwt, is dat van de "slimme steden". Volgens de visionairen van Intel en Cisco zullen onze laptop, GSM, horloge, wekker,... weldra samenwerken om onze dagdagelijkse taken optimaal te ondersteunen. Onze auto's zullen ons waarschuwen voor gevaren, terwijl de reclame langs de weg gepersonaliseerd zal worden aan onze huidige noden.

mogelijk om de verschillende detectoren parallel te laten werken en niet langer sequentieel. Dit leidt ook tot de mogelijkheid om de communicatie die de verschillende mechanismen versturen te bundelen in één bericht, waardoor het herhaaldelijk gebruik van het draadloze netwerk tot een minimum gereduceerd wordt en de broodnodige optimalisatie van het energieverbruik gerealiseerd kan worden.
Het samennemen van verschillende detectoren en het combineren van communicatie zijn slechts twee van de mogelijkheden. Zo kan ook het geheugengebruik geoptimaliseerd worden door het delen van veranderlijke gegevens tussen detectoren mogelijk te maken. Ook wordt het dankzij codegeneratie mogelijk om een aantal aspecten om te zetten in meer technische code, waar een menselijke programmeur dikwijls voorrang geeft aan leesbaarheid en onderhoudbaarheid.

De toekomst

De noden en mogelijkheden van inbraakdetectie enerzijds en van draadloze sensornetwerken anderzijds, zijn elkaars concurrenten. Draadloze sensorknopen zijn enorm beperkt in hun mogelijkheden en de impact van een degelijke inbraakbeveiliging hypothekeert nagenoeg de volledige functionaliteit van de knoop.
Ofschoon de fysieke toegankelijkheid van sensorknopen leidt tot een situatie waar het feitelijk onmogelijk is om een inbraak te detecteren, blijft het belangrijk om deze netwerken toch te voorzien van een vorm van inbraakdetectie. Hoe meer aanvallen een netwerk van zulke knopen kan detecteren, hoe moeilijker het wordt voor een aanvaller om zich vlot meester te maken van het netwerk en er malafide praktijken mee te ondersteunen.
Naast het onderzoeken van aanvallen en het beschrijven van mechanismen om deze te detecteren, is er nog een andere piste die bewandeld kan worden. Domeinspecifieke talen en codegeneratie kunnen aangewend worden om de consequenties die de implementatie van inbraakbeveiliging met zich meebrengt te verlichten.
Aan de hand van codegeneratie kunnen de detectieprocedures onafhankelijk beschreven worden en toch zo georganiseerd worden dat de uitvoeringstijd geminimaliseerd wordt. Verder wordt ook het gebruik van de netwerkcommunicatie gegroepeerd in een enkele gebundelde zending van de informatie van alle verschillende procedures samen.
Zo resulteert deze aanpak in een automatisering van de implementatie van inbraakdetectiemechanismen, waardoor de flexibiliteit om code te organiseren behouden blijft en het mogelijk wordt om de impact van deze bijkomende niet-functionele code te minimaliseren. De onafhankelijkheid van de domeinspecifieke taal biedt verder de mogelijkheid om platformonafhankelijke beschrijvingen van inbraakdetectiemechanismen te hanteren binnen het heterogene landschap van de draadloze sensornetwerken.

Zo heeft de ontwikkelaar van de software van de sensorknopen die weldra alomtegenwoordig zullen zijn in onze huizen, alvast de mogelijkheid om snel eneffectief meerdere inbraakdetectiemechanismen toe te voegen aan zijn eigen functionele code. Laat ons hopen dat we op die manier morgen met een gerust hart een fles melk uit de koelkast kunnen blijven nemen.

Christophe Van Ginneken studeert computerwetenschappen aan de KU Leuven