Cybersecurity is een groot maatschappelijk probleem. Digitale inbraken in kritische systemen, zoals elektriciteitsnetten of banken, staan meer en meer in de belangstelling. En door onze toenemende afhankelijkheid van elektronica wordt het waarborgen van de privacy van gebruikers steeds belangrijker. Prof. dr. Sandro Etalle werkt aan de technische universiteiten van Eindhoven en Twente aan beveiliging die criminelen een stap voor blijft. *Door Sonja Knols*

Kwaadwillenden een stap voor zijn

Sandro Etalle is voorzitter van de mede door CeDICT (Centre for Dependable ICT Systems van de 3TU Federatie) gefinancierde security groep aan de TU/e. Hij werkt één dag per week bij de groep Distributed and Embedded Security van de UT. Etalle heeft samen met Damiano Bolzoni en Emmanuele Zambon aan de UT het bedrijf Securitymatters opgericht, dat momenteel onder andere wordt gefinancierd door een Valorisation Grant van STW.

Grotendeels onbewust ben je de hele dag draadloos aan het communiceren met je omgeving. Je mobieltje in je zak wordt uitgepeild door antennes en klantenkaarten verraden wanneer je waar welk product hebt gekocht. ‘We gooien onze privacy met bakken buitenboord’, zegt hoogleraar computerbeveiliging Sandro Etalle enigszins onheilspellend in zijn werkkamer op de TU/e. ‘Security-onderzoekers zoals ik willen ervoor zorgen dat je identiteit niet gestolen kan worden.’ Daarnaast worden kritische systemen zoals de energievoorziening door de toenemende automatisering steeds kwetsbaarder voor cybercriminaliteit. ‘Ik krijg steeds meer werk’, lacht hij.

Inbraak in streepjescode

Etalle houdt zich bezig met een veelheid aan onderwerpen. Zo werkt hij binnen het Eindhoven Institute for the Protection of Systems and Information (EIPSI) aan de veiligheid van RFID-systemen. ‘Van RFID (Radio Frequency IDentification) wordt veel verwacht. Op termijn zouden RFID-chips streepjescodes moeten gaan vervangen. Dat betekent dat je ze heel goedkoop moet kunnen produceren. Een volwaardige processor past er niet in, en ze bevatten geen batterijen. Ondertussen kun je ze van een afstand wel

Sentinels

Sentinels is een programma van Technologiestichting STW, de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) en het ministerie van Economische Zaken, Landbouw en Innovatie. Sentinels houdt zich bezig met alle aspecten van beveiliging van computersystemen en computernetwerken. Daarbij gaat het zowel om ontwerp en ontwikkeling als beheer van veilige systemen. Ook streeft het programma naar kwaliteitsverhoging en kostenbesparing op deze gebieden. Het totale budget bedraagt ongeveer tien miljoen euro. Het programma is gestart in 2004 en heeft een looptijd van acht jaar. Er wordt inmiddels druk nagedacht over een vervolg, dat aansluit bij de nieuwe vragen en mogelijkheden.

uitlezen, waardoor je groot risico loopt dat je bijvoorbeeld onbewust getraceerd wordt. Die chips beveiligen, op een manier die weinig rekenkracht en energie kost, dat is de uitdaging', vat Etalle samen.
De gevolgen van ongewenst meekijken kunnen fors zijn. 'Stel je voor dat die RFID-chips inderdaad overal terechtkomen. In de producten uit de supermarkt, in je kleding. Dan is het alsof je rondloopt met een streepjescode, die overal kan worden gelezen. Op die manier kan iemand erachter komen of je ergens bent of bent geweest. Het waarborgen van de privacy van de gebruiker is dus een van de belangrijkste doelen.' Maar niet alleen voor individuen is het belangrijk dat de chips inbraakproof zijn. Ook bedrijven kunnen er nadelen van ondervinden als RFIDs traceerbaar zijn door onbevoegden. Een bedrijf dat RFIDs bijvoorbeeld gebruikt om zijn producten te volgen, kan ongewild veel informatie prijsgeven over zijn logistieke processen. En daarmee kan het zijn voordeel ten opzichte van de concurrent verliezen.

Steeds in beweging

Etalle noemt de immer voortschrijdende technologie en de daarbij behorende nieuwe manieren van mogelijk misbruik de grootste uitdaging van zijn vak. 'Security is in grote mate een moving target. De fundamenten staan vast, maar de soorten aanvallen zijn steeds weer anders. Toen het op security gerichte subsidieprogramma Sentinels in 2004 begon (zie kader), hadden we vooral te maken met hackers die zich op besturingssystemen richtten. Nu vechten we tegen geavanceerde systemen zoals de worm Stuxnet, die cruciale infrastructuur aanvalt en zeer waarschijnlijk is gemaakt door een overheidsorganisatie.' Daarnaast maakt de toenemende automatisering het steeds belangrijker dat er in een vroeg stadium wordt nagedacht over security-aspecten. Etalle noemt als voorbeeld de automotive industrie: 'Auto's worden steeds meer bestuurd door computers. Stel je voor dat iemand die computer hackt en er op afstand voor zorgt dat de auto niet meer kan rijden... Ons onderzoek is dus niet alleen intellectueel heel uitdagend, maar ook heel relevant.'
ICT-beveiligingsproblemen kunnen vergaande consequenties hebben voor de maatschappij. 'Voor de energievoorziening gaan we toe naar elektronische meterkasten bij mensen thuis. Als je die op afstand kunt lezen, doemen er ook mogelijkheden tot misbruik op. Stel je voor dat je alle elektriciteit in Eindhoven op hetzelfde moment afsluit en weer aanzet, dan ligt het hele netwerk plat.' En als terroristen inbreken in de centrale besturing van een kerncentrale, zijn de gevolgen helemaal niet te overzien.

Twee aanvalsroutes

Er zijn twee manieren om dit soort misbruik te voorkomen. Vroeg in de ontwikkeling van nieuwe technologie kun je er aan de engineeringkant voor zorgen dat een systeem moeilijker gekraakt kan worden. 'Dat proberen we nu dus met die RFID-chips. We ontwikkelen bijvoorbeeld nieuwe protocollen die de privacy garanderen.' Daarvoor maakt Etalle dankbaar gebruik van de expertise van zijn cryptografie-collega's binnen het EIPSI-instituut.
De tweede manier is om er achteraf voor te zorgen dat een systemen niet gehackt wordt. Dat kan door aanvallen vroegtijdig te detecteren en af te wenden. Hiervoor ontwikkelde de van oorsprong Italiaanse hoogleraar samen met zijn collega's van de UT een nieuw type netwerkinbraakdetectiesysteem, dat – naast de bestaande virusscanners, spywaredetectieprogramma's en firewalls – een extra beschermende schil om een netwerk heen legt. 'Dat is vooral interessant voor bedrijven die services aanbieden op internet. Denk bijvoorbeeld aan banken, waar bepaalde computers gebruikt worden voor internetbankieren. Maar ook aan systemen die onze kritische infrastructuur beheren (elektriciteit, water, gas). Die moet je tot op het hoogste niveau beschermen.'

'We gooien onze privacy met bakken buitenboord'

Afwijkend gedrag

Het systeem, dat Etalle met zijn compagnons binnen het spin-off bedrijf SecurityMatters ontwikkelt, detecteert aanvallen op netwerkprotocollen. Uniek is dat het niet werkt met een zwarte lijst van bekende aanvallen, maar dat het gebaseerd is op afwijkend gedrag van het netwerk in kwestie. Zo kan het ook compleet nieuwe *zero-day* aanvallen herkennen. 'We zijn nu potentiële aanvallers eens een stapje voor', glimlacht Etalle trots. Meestal moet een nieuwe aanval namelijk eerst worden beschreven. Pas als hij in een databank is geladen, kan een beveiligingsysteem hem herkennen en afweren. Ondertussen kunnen de inbrekers hun werkwijze alweer hebben aangepast. Etalle: 'Het mooie van ons systeem is dat het voor criminelen onmogelijk is om het voor te zijn, omdat het zich aanpast aan zijn omgeving. Dus zelfs als zij de software hebben, kunnen ze niet weten welke aanvallen in een specifieke omgeving wel en niet herkend zullen worden.' Dit komt omdat de beveiliging eerst kijkt hoe het netwerk in kwestie normaal functioneert, en vervolgens afwijkend gedrag opmerkt. Om te snappen wat als aanval wordt beschouwd, zou je als kwaadwillende de software eerst moeten testen op het systeem waarin je wilt inbreken. Etalle: 'Het spel aanvaller-verdediger is altijd in het voordeel van de aanvaller. Maar nu weet de aanvaller eens niet wat zich bij de verdediger afspeelt. Dat is een klein maar belangrijk stapje voorwaarts.' I/O

One step ahead of attackers

Prof. dr. Sandro Etalle works on different aspects of security: protecting computers and networks against violent attacks. For example, he and his co-workers from Eindhoven University of Technology work on new protocols for RFID tags to prevent identity theft and misuse of stored data. Furthermore, within their spin-off company Securitymatters from the University of Twente, he and his colleagues developed a new network intrusion detection system. This system is anomaly-based instead of signature-based. In the latter case the system can only recognise attacks which have been previously disclosed, analysed and whose signature has been loaded into the system. The new anomaly-based system analyses the normal behaviour of the network, and identifies all abnormal behaviour as a possible attack. Since potential hackers don't know beforehand what type of attack the system will classify as abnormal, defence is one step ahead of the attackers.