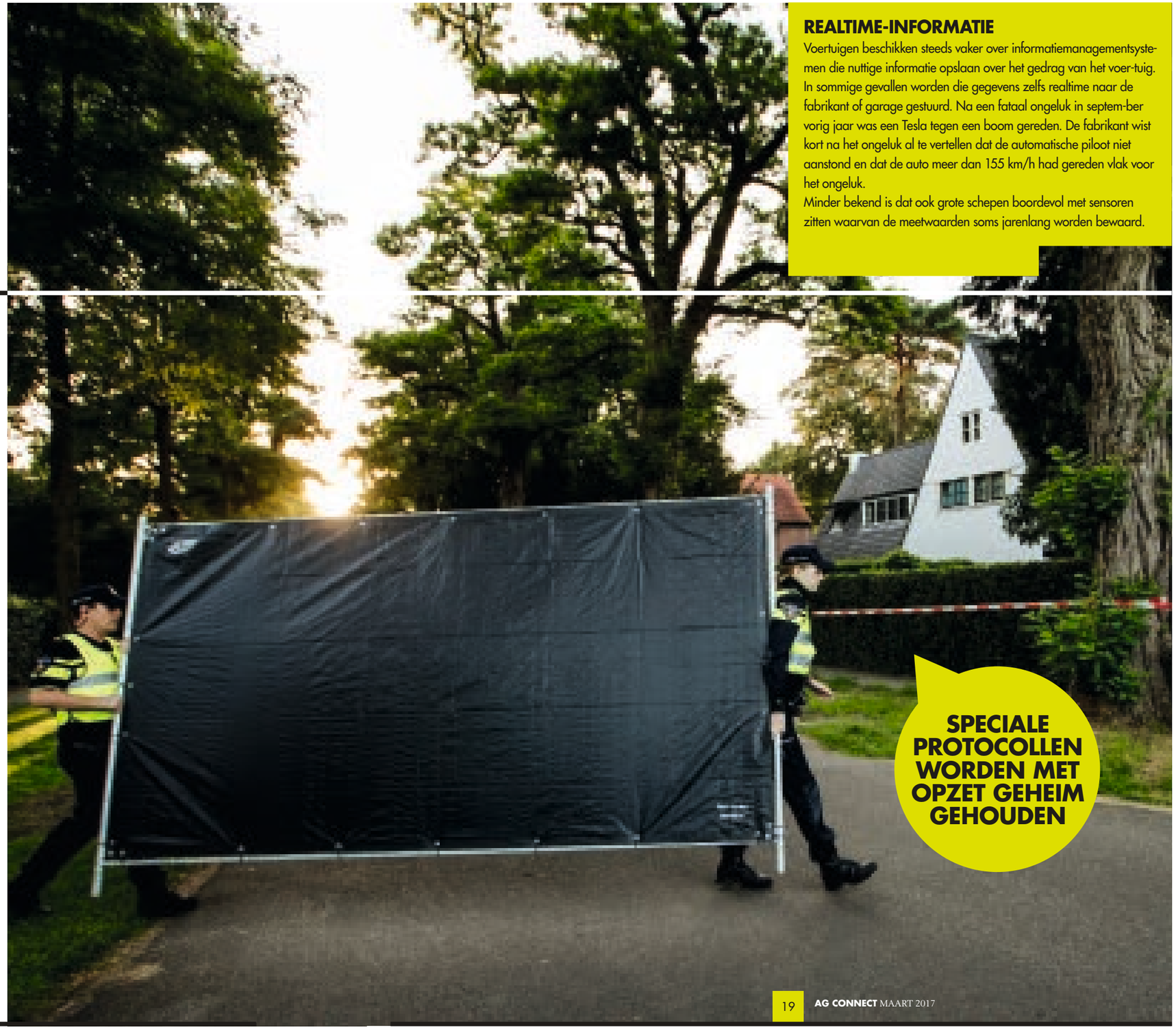
FORENSISCH ONDERZOEK IN DE TIJD VAN INTERNET OF THINGS

NIEUWE TECHNIEKEN, ONGEKENDE MOGELIJKHEDEN

HET INTERNET OF THINGS BEVAT EEN SCHAT AAN INFORMATIE VOOR FORENSISCH ONDERZOEK. MAAR DIE LIGT NIET VOOR HET OPRAPEN. OVERHEID EN BEDRIJFSLEVEN ZULLEN MOETEN INVESTEREN IN SPECIALE APPARATUUR EN IN OPLEIDINGEN VOOR HET TOEPASSEN VAN NIEUWE TECHNIEKEN.

door Hans Henseler

VOLGENS HET OPENBAAR MINISTERIE KOMEN DE GEGEVENS VAN DE STAPPENTELLER OP DE TELEFOON VAN DE VERDACHTE VAN DE MOORD OP KOEN EVERINK NIET OVEREEN MET HET VERHAAL VAN DE VERDACHTE. De verdachte claimt namelijk dat hij rond de moord is ontvoerd door de daders. De advocaat van de verdachte vindt het 'gevaarlijk' om conclusies te trekken uit de gegevens van de stappenteller.
Wat weten we eigenlijk over de bewijskracht van dit soort gegevens, die in hoog tempo door allerlei apparaten bewust en onbewust over ons gedrag worden bijgehouden? Van mobiele telefoons is al langer bekend dat ze een rijke bron van informatie zijn in strafrechtelijke onderzoeken. Door het persoonlijke karakter van de mobiele telefoon en door de sociale media-apps krijgen dit soort digitale sporen steeds meer het karakter van klassieke



SPECIALE PROTOCOLLEN WORDEN MET OPZET GEHEIM GEHOUDEN

REALTIME-INFORMATIE

Voertuigen beschikken steeds vaker over informatiemanagementsystemen die nuttige informatie opslaan over het gedrag van het voer-tuig. In sommige gevallen worden die gegevens zelfs realtime naar de fabrikant of garage gestuurd. Na een fataal ongeluk in septem-ber vorig jaar was een Tesla tegen een boom gereden. De fabrikant wist kort na het ongeluk al te vertellen dat de automatische piloot niet aanstond en dat de auto meer dan 155 km/h had gereden vlak voor het ongeluk.
Minder bekend is dat ook grote schepen boordevol met sensoren zitten waarvan de meetwaarden soms jarenlang worden bewaard.

SYMPOSIUM E-DISCOVERY

Op 11 april vindt het 8ste Symposium E-Discovery in Nederland plaats in Leiden. Het thema is dit jaar het Internet of Things. Het symposium wordt georganiseerd door het lectoraat Digital Forensics & E-Discovery van de specialisatie Forensisch ICT van de Hogeschool Leiden i.s.m. kenniscentrum Create-IT van de Hogeschool van Amsterdam. Na de aanslagen in Parijs, Brussel en Berlijn is het thema smart cities en safety & security zeer actueel. Het IoT speelt daarin een belangrijke rol en het symposium begint met een keynote over het Antwerp City-of-Things-project. Informatie over het programma is te vinden op: www.hsleiden.nl/symposium-ediscovery. Deelnemen is gratis, registratie is vereist.

forensische sporen, zoals vingerafdrukken en DNA.

GEHEIM

Iedereen begrijpt dat een stappenteller iets zegt over de bewegingen van de drager. Maar minder bekend is dat een telefoon continu op zoek is naar bekende draadloze wifinetwerken. Het gevolg is dat in het geheugen van draadloze routers van onbekende

Beveiligingsexperts adviseren de UPnP-functie uit te schakelen

wifinetwerken (tijdelijk) de lijst van netwerknamen wordt opgeslagen die door een passerende smartphone, tablet of laptop worden uitgezonden, zodra een wifinetwerk in de buurt is.
Wat te denken van de smart-tv's en pratend speelgoed dat meeluistert naar alles wat we hoorbaar met elkaar bespreken? De slimme thermostaat, de online-(brand-)alarminstallatie, videocamera's, slimme stekkers en zelfs onlinekookapparaten die via internet gevolgd en bestuurd kunnen worden.
Al die apparaten praten via speciale protocollen die op dit moment nog vaak fabrikantspecifiek zijn en met opzet geheim worden gehouden om concurrentie te verhinderen.
Uiteindelijk willen al deze slimme apparaten toegang tot het internet en is het van belang voor de fabrikanten dat de installatie ervan zo gebruiksvriendelijk mogelijk is. Daarom is het UPnP-(Universal Plug and Play)-protocol bedacht. Dit is een verzameling van netwerkprotocollen die slimme apparaten in staat stellen om elkaars aanwezigheid te detecteren en samen te werken.
Dit klinkt geweldig, maar gebruikers realiseren zich niet dat bijvoorbeeld een nieuwe ip-bewakingscamera op eigen houtje firewallregels aan de router toevoegt om zichzelf bereikbaar te maken op het internet. Beveiligingsexperts adviseren dan ook om de UPnP-functie in de routers uit te schakelen. Het gevolg daarvan is natuurlijk wel dat het aansluiten van nieuwe apparatuur problemen kan geven die niet door de gemiddelde consument opgelost kunnen worden.

SLECHTE BEVEILIGING

De internetzoekmachine Shodan is gespecialiseerd in het ontdekken van apparaten in het Internet of Things die door gebruikers niet of slecht zijn beveiligd. Zo werd in november vorig jaar bekend dat honderden pagina's uit vertrouwelijke terrorismedossiers van politiedienst Europol zijn gelekt. De oorzaak was een medewerker die het dossier thuis op een netwerkschijf had opgeslagen die verbonden was met het internet, zonder wachtwoord.
De slechte beveiliging van slimme apparaten is niet alleen een probleem voor de eigenaren. Hackers weten handig gebruik te maken van de beveiligingslekken en installeren malware zodat de apparatuur onderdeel wordt van een botnet waarmee cyberaanvallen gelanceerd kunnen worden (zie kader Risico's). Bij een cyberaanval is dus niet zonder meer duidelijk of de eigenaar verantwoordelijk is voor het misbruik.
Naarmate we meer vertrouwen op slimme apparaten om ons heen, is het belangrijk om beter te begrijpen wat die apparaten precies doen en hoe ze op elkaar reageren. Bedrijven houden uit concurrentieoverwegingen de gebruikte protocollen en bestandsformaten met opzet geheim. Kennis van firewalls, besturingssystemen, zero-day exploits en internetprotocollen is dan niet meer toereikend. Om toch inzicht te krijgen in de werking en eventueel onverwachte bijwerkingen, zijn speciale digitale forensische onderzoeksmethodes en opleidingen nodig.

OPLEIDINGEN

Bij gebrek aan open standaarden en standaardcomponenten, zal forensisch onderzoek aan het IoT gebruik moeten maken van protocolanalyse om de werking van het IoT-netwerk te doorgronden en van JTAG, chip off en ISP digital forensics voor analyse van de werking en dataopslag. Via JTAG (Joint Test Action Group) wordt gebruik gemaakt van testprotocollen om gegevens te verkrijgen. Bij chip off wordt een geheugenchip zodanig geprepareerd dat het geheugen rechtstreeks wordt uitgelezen. Met behulp van ISP (In System Programming) kunnen onderzoekers rechtstreeks een geheugendump maken zonder chip off.
Het IoT bevat een schat aan informatie voor forensisch onderzoek, maar die ligt niet zomaar voor het oprapen. Overheid en bedrijfsleven zullen moeten investeren in speciale apparatuur. En opleidingen moeten studenten opleiden en bijscholing aanbieden in het toepassen van deze nieuwe technieken. Daarbij zal alleen theorieles niet toereikend zijn, maar moet er geïnvesteerd worden in laboratoria waar de hardware aan een digitaal forensisch onderzoek onderworpen kan worden.

AUTEUR

HANS HENSELER is lector Digital Forensics & E-Discovery bij de specialisatie Forensische ICT aan de Hogeschool Leiden en algemeen directeur en medeoprichter van Tracks Inspector.

SERIEUZE VEILIGHEIDSRISICO'S

Slecht beveiligde slimme apparaten die aan het internet zijn gekoppeld, vormen een serieus risico voor de veiligheid op internet. In september vorige jaar werd een grootschalige denial of service attack gelanceerd. De malware 'Mirai' verspreidt zich over kwetsbare apparaten door constant het internet te scannen op zoek naar aangesloten slimme apparaten die beschermd zijn met default-wachtwoorden en gebruikersnamen.

Zo kunnen botnets met meer dan een miljoen nodes ontstaan die ingezet kunnen worden zonder dat de eigenaren vermoeden wat er aan de hand is. De consequentie is dat bij het interpreteren van sporen in slimme apparaten het nodig is om te onderzoeken wie er verantwoordelijk is voor de aanwezigheid van bepaalde data.

Overigens zit het risico niet alleen in de georganiseerde (cyber) criminaliteit. Ook landen houden zich bezig met het hacken van (kritieke) infrastructuren. Denk aan Stuxnet en aan de meer recente onthulling van Snowden in Wikileaks, waaruit bleek dat Britse geheimagenten toegang hadden tot de systemen van Belgacom, waardoor ze eenvoudig gesprekken konden afluisteren.

Sinds een paar jaar is nu ook duidelijk dat bedrijven frauderen met computersystemen. Denk daarbij aan de sjoemelsoftware van Volkswagen waarmee geknoeid was om ervoor te zorgen dat tijdens testen de auto binnen de gestelde emissienormen zou blijven. Inmiddels worden andere autofabrikanten ook verdacht van vergelijkbare fraude. Veel feiten over de toedracht van deze fraude zijn bekend geworden na grootschalige e-mailonderzoeken, maar alleen door het decoderen van de interne machinecode kan de exacte werking van de fraude worden aangetoond.

REACTIES EN BIJDRAGEN

Voor reacties en nieuwe bijdragen van IT-experts:
Henk Ester
020-2356415
h.ester@agconnect.nl