Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie
ISSN: (Online) 2222-4173, (Print) 0254-3486

’n Bestekopname van slimhuistegnologie vir sekuriteitsdoeleindes in Suid-Afrika

Outeur:
Burgert A Senekal

Affiliasie:
Departement Rekenaarwetenskap en Informatika, Universiteit van die Vrystaat, Suid-Afrika

Korresponderende outeur:
Burgert A Senekal
Epos:
burgertsenekal@yahoo.co.uk

Datums:
Ontvang: 06/07/21
Aanvaar: 06/10/21
Gepubliseer: 25/11/21

Hoe om hierdie artikel aan te haal:
Burgert A Senekal, ’n Bestekopname van slimhuistegnologie vir sekuriteitsdoeleindes in Suid-Afrika, *Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie* 40(1) (2021). https://doi.org/10.36303/SATNT.2021.40.1.856

Alhoewel slimhuistegnologie sedert die 1970’s bekend is, het dit onlangs in gewildheid toegeneem namate die tegnologie goedkoper en meer gebruikersvriendelik geword het. Digitale assistente, byvoorbeeld Amazon Alexa, Google Assistant en Apple Siri, is ook onlangs by hierdie sisteme geïntegreer, wat verdere toepassingsmoontlikhede geskep het. Die huidige studie ondersoek die potensiaal van hedendaagse slimhuistegnologie om mense se veiligheid te verbeter. Beheerstelsels soos Amazon Echo, Google Nest en Apple Homekit word bespreek, tesame met toegewyde slimhuis-sekuriteitstelsels soos Ajax en Hikvision AX PRO. Radioprotokolle en sommige sensors word ook ondersoek, met ’n spesifieke klem op hulle vermoëns en gebreke. Laastens word ’n aanbeveling gemaak en ’n voorbeeld van ’n toepassing vir veiligheidsdoeleindes word in Apple se Homekit met behulp van Apple se Shortcuts saamgestel.

Kernwoorde: Amazon Alexa; Amazon Echo; Apple Homekit; Apple Siri; Google Assistant; Google Nest; kunsmatige intelligensie; slimhuise; huisoutomatisering

An overview of smart-home technology for security purposes in South Africa: Although smart-home technology has been in use since the 1970s, it has recently increased in popularity as the technology has become cheaper and more user-friendly. Digital assistants such as Amazon Alexa, Google Assistant and Apple Siri have also recently been integrated with these systems, which has created further application possibilities. The current study examined the potential of today’s smart-home technology to improve people’s safety. Control systems such as Amazon Echo, Google Nest and Apple Homekit are discussed, along with dedicated smart-home security systems such as Ajax and Hikvision AX PRO. Radio protocols and some sensors were also examined, with specific emphasis on their capabilities and shortcomings. Finally, a recommendation is made and an example of an application for security purposes is compiled in Apple’s Homekit using Apple’s Shortcuts.

Keywords: Amazon Alexa; Amazon Echo; Apple Homekit; Apple Siri; Google Assistant; Google Nest; artificial intelligence; smart homes; home automation

Inleiding

Misdaad bly ’n probleem in Suid-Afrika. Alhoewel die per capita-moordsyfer in die middel-1990’s ’n hoogtepunt bereik het, dui amptelike syfers daarop dat beide die getal moorde en per capita-moorde sedert 2011 toegeneem het (United Nations Office on Drugs and Crime, 2020; World Bank, 2020). Suid-Afrika bly steeds een van die gevaarlikste lande ter wêreld, met ’n totaal van 527 337 mense wat vanaf 1994 tot 2019 teen ’n gemiddelde van 20 282 per jaar vermoor is (United Nations Office on Drugs and Crime, 2020). Boonop het die jaarlikse aangetekende voorvalle van roof by residensiële en nieresidensiële persele gedurende die afgelope twaalf jaar toegeneem (Adam, 2021).

Slimhuistegnologie het oor die afgelope paar jaar in gewildheid toegeneem en bied ’n oplossing om mense se veiligheid te verbeter. Slimhuistegnologie sluit gewoonlik ’n verskeidenheid sensors in wat deur middel van ’n slimfoontoepassing geïntegreer kan word, kennisgewings uitstuur wanneer ’n bedreiging geïdentifiseer word, en selfs aksies neem deur ligte aan en af te skakel, slotte oop en toe te sluit en blindings en gordyne oop en toe te maak. Die gewildste slimhuisplatforms is Amazon Echo, Google Nest en Apple Homekit, wat onderskeidelik digitale assistente deur Amazon Alexa, Google Assistant en Apple Siri insluit (Einarsson et al., 2017; Fifield, 2020; Hearn, 2020; Kinsella, 2020; Yoffie et al., 2018). Teen 2018 het 41% van huise in die VSA gebruik gemaak van Amazon Alexa of Google Assistant (Weaver et al., 2020) en

teen 2020 het Amazon 53% van die slimluidsprekermark in die VSA besit, Google 30,9% en Apple 2,8% (Kinsella, 2020). Die huidige studie ondersoek die moontlikhede om slimhuistegnologie vir sekuriteitsdoeleindes in Suid-Afrika aan te wend. Omdat verskeie outeurs Amazon, Google en Apple uitlig as die markleiers, word daar op hierdie platforms gefokus, maar ander slimsekuriteitsplatforms soos Hikvision AX Pro en Ajax word ook betrek. Laasgenoemde twee is gekies omdat Hikvision (2021b) self hulle eie radioprotokol met Ajax s'n vergelyk, benewens 'n vergelyking met slimhuis-kommunikasiesisteme wat binne Amazon, Google en Apple funksioneer. Die doel van die huidige studie is om 'n bestekopname van slimhuistegnologie vir sekuriteitsdoeleindes te onderneem, ondersoek in te stel na hoe die mark tans daaruit sien en hoe sisteme geïntegreer kan word.

Agtergrond

'n Definisie van slimhuise

Verskeie definisies van slimhuise bestaan in die literatuur, soos onder andere bespreek in Marikyan et al. (2019) en Sovacool en Furszyfer Del Rio (2020). Breedweg verwys slimhuistegnologie na sisteme waar 'n verskeidenheid sensors en toestelle in 'n privaat woning deur middel van 'n internetverbinding gekoppel word (Bugeja, 2021). Marikyan et al. (2019) omskryf slimhuistegnologie soos volg:

> Die slimhuis verteenwoordig slimtoestelle en sensors wat geïntegreer is in 'n intelligente stelsel, wat bestuur, monitering, ondersteuning en responsiewe dienste bied en 'n reeks ekonomiese, sosiale, gesondheidsverwante, emosionele, volhoubaarheids- en sekuriteitsvoordele bied (kyk ook Liu et al., 2019; Albģstroiu et al., 2021).

Robles en Kim (2010), Stanley (2019) en Bugeja (2021) skryf dat slimhuise sover terug as 1975 dateer toe 'n Skotse maatskappy X10 ontwikkel het. Dit het versoenbare toestelle in staat gestel om oor die bestaande elektriese bedrading in 'n huis met mekaar te kommunikeer. Sovacool en Furszyfer Del Rio (2020) noem egter dat die konsep so ver terug as die laat-1800's strek en dat Thomas Edison self in 1910 gekleurde gloeilampe gepatenteer het. Die term "slimhuis" ("smart home") dateer uit 1984, toe dit deur die American Association of House Builders geskep is (Bugeja, 2021). Saam met slimhuise het stem-geaktiveerde digitale assistente ontwikkel om slimhuise te bestuur, maar dit was eers met die ontwikkeling van hoëspoedverwerkers, kunsmatige intelligensie en die beskikbaarheid van groot datastelle dat digitale assistente oor die afgelope dekade 'n alledaagse verskynsel geword het (Yoffie et al., 2018). Hierdie tegnologie is nog baie nuut, met Amazon Alexa vir slimhuise wat in 2014 bekendgestel is en Google Assistant in 2016. Apple Siri is eers sedert 2018 by Apple Homekit geïntegreer (Bugeja, 2021; Yoffie et al., 2018).

Dit is belangrik om daarop te let dat die tipiese gebruikers van slimhuistegnologie nie kenners van rekenaarprogrammeringstale is nie en eerder leketegnologie-entoesiaste is. Bu et al. (2018) skryf byvoorbeeld dat die gebruikersbasis van huisoutomatisering grootliks bestaan uit niekundiges wat 'n onvoldoende agtergrond met die programmering van hibriede beheerstelsels het. Slimhuistegnologie word derhalwe ontwikkel om gebruikersvriendelik te wees, en die eenvoud waarmee sisteme geïntegreer kan word, speel 'n belangrike rol in die opname van hierdie tegnologie.

Die volgende afdeling bespreek sommige toepassings van slimhuistegnologie.

Soorte slimhuise

De Silva et al. (2012) en Marikyan et al. (2019) identifiseer vier soorte slimhuise: slimhuise wat dienste lewer, slimhuise wat data insamel, slimhuise wat toesig hou en slimhuise wat energie bespaar. Die huidige afdeling bespreek hierdie verskillende toepassings van slimhuistegnologie.

Slimhuistegnologie word in 'n verskeidenheid studies ondersoek as ondersteuning vir bejaardes en gestremdes (Demiris en Hensel, 2008; Liu et al., 2019; Patel et al., 2012; Peetoom et al., 2015). Slimhuistegnologie kan byvoorbeeld bejaardes of gestremdes ondersteun deur hulle te herinner om medikasie te neem, krane outomaties toe te draai, bewegings te monitor, of deur familielede deur middel van kameras toe te laat om kwesbare persone te monitor. Op hierdie manier kan slimhuistegnologie kwesbare persone toelaat om langer onafhanklik te woon (Liu et al., 2019). De Silva et al. (2012) stel ook voor dat kinders só gemonitor kan word om ongelukke te voorkom, terwyl Maras (2015) toestelle noem wat babas kan monitor. Slimhuise kan ook gebruik word om mense se emosionele welstand te verbeter en die slimhuis-ligsisteem, Philips Hue, is reeds in 'n verskeidenheid studies vir hierdie doel gebruik (Capodieci et al., 2018; Clark en Dutta, 2015; Davis et al., 2015; Ly et al., 2016).

Slimhuise wat data insamel, kan alledaagse gebeure in mense se lewens opteken. De Silva et al. (2012) noem die voorbeeld van 'n kind se eerste tree, wat gewoonlik nie op kamera vasgelê kan word nie omdat dit onverwags is. Hierdie soort slimhuise verg egter 'n groot aanpassing van gebruikers omdat dit die privaatheid van die inwoners van die huis ondermyn (Marikyan et al. 2019).

Slimhuise wat toesig hou, word gewoonlik vir sekuriteitsdoeleindes aangewend (Marikyan et al., 2019) en veiligheidsisteme is die tweedegrootste komponent van die slimhuismark naas vermaak (Yoffie et al., 2018). Een van die grootste voordele van slimhuissisteme is dat dit sekuriteit verbeter deur middel van kameras, bewegingsensors en deur- en vensterkontakte. Boonop integreer slimhuistegnologie hierdie sensors binne 'n beheersisteem wat met 'n slimfoontoepassing opgestel en gemoniteer kan word. Alhoewel slimhuistegnologie vir sommige mense om gerief gaan, is dit nie slegs daartoe beperk nie:

> Indien dit op die regte manier opgestel word, is slim huise nie net "'n lekker om te hê" nie. Hulle bied uitstekende sekuriteit, in die vorm van 'n standaarddief- of brandalarm, outomatiese deursluit en oopsluit, outomatiese skakel van polisie en brandweerdienste en slim beligting (Anoniem, 2019b).

Slimhuissisteme kan ook gebruik word om energie te bespaar (Hosseini et al., 2017; Sovacool en Furszyfer Del Rio, 2020). Daar is wêreldwyd 'n poging om energieverbruik te verminder en 'n skuif na groen energie soos son- en windkrag (Marikyan et al., 2019), maar groen energie verg tans 'n groot kapitaaluitleg (Longe et al., 2019). Een manier om koste te bespaar, is om energieverbruik te verminder, wat beteken dat 'n kleiner son- en/of windkragsisteem benodig word. Slimhuistegnologie bring energiebesparings mee, omdat ligte outomaties aan- en afskakel soos benodig, klimaatbeheer kan aangepas word by die persoon wat in 'n vertrek teenwoordig is, en energieverbruik kan outomaties gemonitor word.

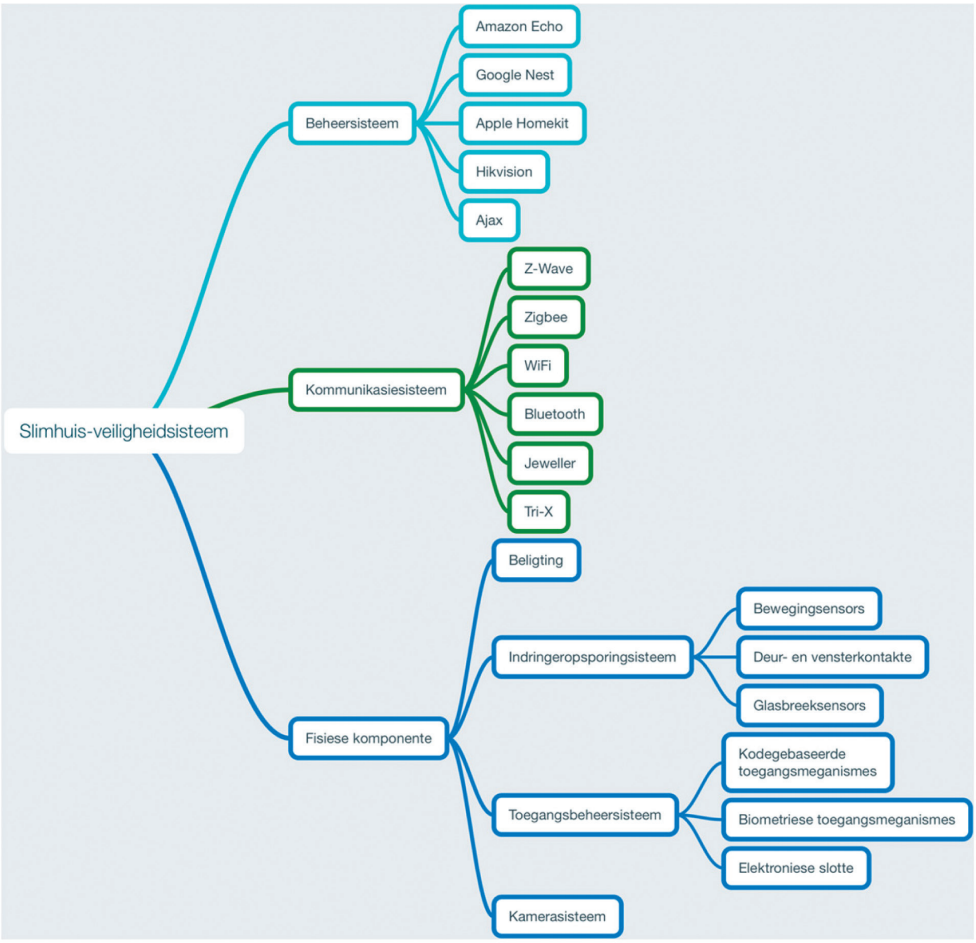
Gebruikers is natuurlik nie beperk tot een of ander toepassing van slimhuistegnologie nie: dieselfde kamera wat gebruik word om kinders te monitor, kan ook byvoorbeeld die huis vir veiligheidsdoeleindes monitor, soos dieselfde bewegingsensors wat vir energiebesparing aangewend word, ook indringers kan identifiseer. Slimhuise is met ander woorde veeldoelig, alhoewel die huidige artikel op slimhuise vir veiligheidsdoeleindes fokus.

Die volgende afdeling bespreek die komponente van 'n slimhuissisteem.

'n Slimhuis-veiligheidsisteem

Slimhuissisteme bestaan uit drie primêre tegnologie-afdelings: fisiese komponente (sensors en aandrywers) wat die data waarneem, die beheersisteem wat data van die fisiese komponente ontvang en besluite neem, en die kommunikasiesisteem wat die fisiese komponente en die beheersisteem verbind (Ammar et al., 2018; Kauranen, 2021; Liu et al., 2019). 'n Slimhuissisteem kan ook vergelyk word met wat die VSA se Department of Homeland Security (2019) 'n elektroniese sekuriteitsisteem noem. Meer spesifiek kan 'n slimhuis-veiligheidsisteem as 'n netwerkbeveiligingsisteem geklassifiseer word wat op een netwerk funksioneer, met drywers vir die verskillende komponente van die subsisteme. Hierdie subsisteme bestaan uit 'n indringeropsporingsisteem, 'n toegangsbeheersisteem en 'n kamerasisteem (Department of Homeland Security, 2019). Wanneer Ammar et al. (2018), Kauranen (2021) en Liu et al. (2019) gekombineer word met die Department of Homeland Security (2019), kan die komponente van 'n slimhuisveiligheidsisteem gekonseptualiseer word soos in figuur 1 getoon word. Die beheer- en kommunikasiesisteme wat in figuur 1 aangedui word, word in die huidige studie ondersoek.

Hierdie indeling word ook in die hieropvolgende bespreking gebruik.



FIGUUR 1: Die komponente van 'n slimhuis-veiligheidsisteem

Beheersisteem

Met inligting wat van die fisiese komponente (soos later in die huidige studie bespreek word) ingesamel word, voer die beheersisteem eenvoudige taakoutomatisering uit, analiseer of voorspel die ligging van die inwoner en hulle gedrag, of identifiseer die gesondheidstatus van 'n inwoner wat by die huis woon (Liu et al., 2019).

Ten opsigte van beheersisteme word die slimhuismark oorheers deur Amazon Echo, Google Nest en Apple Homekit (Einarsson et al., 2017; Fifield, 2020; Hearn, 2020; Kinsella, 2020; Meng et al., 2018; Nield, 2021; Yoffie et al., 2018). Al drie hierdie maatskappye het in 2014 tot die slimhuismark toegetree: Apple het Homekit in 2014 bekendgestel; Google het in 2014 die slimhuismaatskappy Nest bekom en daardeur ook hulle voorneme aangetoon om die slimhuismark te betree, en Amazon het Amazon Echo, hulle slimhuisluidspreker, ook in 2014 bekendgestel (Hilbolling et al., 2019; Stanley, 2019).

Digitale assistente het 'n groot rol in die opkoms van hierdie slimhuissisteme gespeel en Amazon Alexa was sedert 2014 deel van Amazon se slimhuissisteem, terwyl Google Assistant sedert 2016 deel van Google se sisteem (toe bekend as Google Home, tans Google Nest) uitgemaak het. Apple se Siri is in 2018 met Homekit geïntegreer (alhoewel Siri reeds sedert 2011 deel van Apple se iOS uitmaak) (Bugeja, 2021; Hoy, 2018; Stanley, 2019; Yoffie et al., 2018). Amazon Alexa is tans die markleier, en teen 2020 was 7 400 handelsmerke versoenbaar met Alexa, teenoor 1 000 handelsmerke wat met Google Assistant versoenbaar was en 50 handelsmerke wat met Siri versoenbaar was (Weaver et al., 2020).

Al drie hierdie sisteme beheer versoenbare toestelle en bemiddel outomatiserings. 'n Gebruiker kan byvoorbeeld outomaties sy deure sluit wanneer hy die perseel verlaat, deur 'n slimfoontoepassing kontroleer of vensters en deure toe is, videokameras integreer, ensovoorts. Al drie hierdie sisteme het ook sterk en swak punte en gebruikersvoorkeur bepaal watter sisteem gekies word. Hierdie sisteme word in detail in Ammar et al. (2018) bespreek.

'n Deel van wat Apple Homekit se uitbreidingsmoontlikhede beperk, is Apple se streng privaatheidsregulasies, wat hierdie platform die veiligste maak (Hearn, 2020; Yoffie et al., 2018). Nietemin was daar voorheen probleme met sekuriteit, byvoorbeeld 'n man wat ontdek het dat die iPad in sy sitkamer die voordeur sou oopsluit vir almal wat buite gestaan het en Siri gevra het om hulle in te laat (Hoy, 2018). Stute et al. (2021) het ook sekuriteitsgebreke in Apple se infrastruktuur uitgewys. Soos sulke probleme uitgelig word, dateer Apple, Google en Amazon hulle sekuriteit op, en ten tye van die skryf van hierdie artikel sou Siri byvoorbeeld nie sensitiewe inligting gee sonder dat die gebruiker sy foon ontsluit het nie. Stute et al. (2021) meld juis dat hulle hulle bevindinge aan Apple gekommunikeer het en dat Apple daarna hierdie sekuriteitsgebreke hanteer het.

Verskeie slimhuistoepassings bestaan ook om die gebruiker toe te laat om meer dienste binne Amazon Echo, Google Nest en Apple Homekit te integreer. IFTTT ("If This Then That") (https://ifttt.com/) is 'n gewilde toepassing om reëls mee te skep en uit te voer (Bu et al., 2018), en Apple se Shortcuts, wat sedert 2018 in iOS op 'n iPhone of iPad ingebou is, werk op 'n soortgelyke reëlgebaseerde beginsel. Fogli et al. (2017) noem hierdie soort reëls gebeurtenis-voorwaarde-handelingreëls ("event-condition-action" of ECA-reëls) en merk op dat hierdie soort reëls die mees gebruikte paradigma in gebruikerskoppelvlakke vir die konfigurasie en aanpassing van slimhuise deur gebruikers sonder programmeringsvaardighede verteenwoordig (sien ook Bu et al., 2018). Sulke reëlgebaseerde toepassings maak dit byvoorbeeld moontlik om voorwaardes op te stel soos: Indien iemand tuis is en die son reeds ondergegaan het, skakel buiteligte vir twee uur aan.

Sommige toepassings skep ook die geleentheid om 'n paneelbord ("dashboard") te skep, gevisualiseer op 'n Amazon Fire Tablet, Google Nest Hub, Apple iPad of 'n ander monitor, soos byvoorbeeld gekoppel aan 'n Raspberry Pi. Sulke toepassings maak dit dan moontlik om 'n bevelsentrum in die huis te skep waar die weer, die toestand van toestelle, kameras, ensovoorts, op 'n sentrale punt gemonitor en beheer kan word. Voorbeelde van sulke toepassings is Powerhouz (www.powerhouz.com), HomeDash (https://www.homedash.app) of Home Remote (https://thehomeremote.com). Vir gebruikers van Apple Homekit bestaan die moontlikheid ook om van Widgets gebruik te maak wat op die Today-blad van die iPad opgestel word, wat 'n versameling toepassings op een plek integreer. Hierdie metode word later in die huidige artikel toegepas.

Benewens hierdie markleiers bestaan daar ook 'n groot verskeidenheid ander slimhuissisteme, byvoorbeeld Samsung SmartThings, Control4, Yonomi en Allseen (Anderson, 2018; Meng et al., 2018; Nield, 2021), asook toegewyde sisteme wat op sekuriteit fokus, soos Ajax en Hikvision AX PRO.

Ajax is in 2011 gestig en fokus daarop om 'n slim sekuriteitsplatform te wees. Die sisteem voldoen aan verskeie internasionale sekuriteitstandaarde en die spilpunt is daartoe in staat om oor groot afstande (tot 2 000 m) deur middel van Ajax se eie radioprotokol (Jeweller) met sensors te kommunikeer (Ajax, 2021b) (sien volgende afdeling). Alhoewel Ajax nie hulle eie kameras vervaardig nie, kan kameras ook by die sisteem geïntegreer word (Ajax, 2021b). Ajax vervaardig ook slimmuurproppe om toestelle te beheer, wat deur middel van scenario's op hulle toepassing vir outomatisering gebruik kan word (Ajax, 2021a). Dit beteken dat die muurprop byvoorbeeld gebruik sou kon word om ligte outomaties aan te skakel wanneer die alarm geaktiveer word, maar Ajax laat slegs een outomatisering per toestel toe (Ajax, 2021a), wat tot gevolg het dat hierdie

funksionaliteit nie so baie opsies vir die gebruiker sal gee soos wat deur slimhuisstelsels soos Apple Homekit, Google Nest of Amazon Echo beskikbaar is nie.

Hikvision is een van die globale markleiers in sekuriteitsprodukte en is veral bekend vir hulle kameras. In 2020 het Hikvision hulle slim en draadlose alarmplatform, AX Pro, geloods, wat 'n sisteem van draadlose sensors insluit wat deur middel van 'n spilpunt met 'n slimfoon kan kommunikeer (Hikvision, 2020; 2021a). Die sisteem is baie soortgelyk aan Ajax en gebruik ook hulle eie radioprotokol (Tri-X), wat die reikafstand tussen sensors en spilpunte tot bykans twee kilometer vergroot (Hikvision, 2021b) (sien volgende afdeling). Aangesien Hikvision nuut in die slimhuismark is, vervaardig dié maatskappy nog nie so 'n groot verskeidenheid sensors soos Ajax nie.

Die Ajax- en Hikvision-sisteme is nie tans versoenbaar met Apple Homekit, Amazon Echo of Google Nest nie. Dit is 'n groot nadeel van hierdie sisteme, omdat 'n gebrek aan integrasie beteken dat gebruikers wat hierdie platforms gebruik, nie outomatiserings binne hulle bestaande slimhuisplatforms kan insluit nie. Hierdie gebrek aan integrasie kan egter daaraan toegeskryf word dat die sisteme van Amazon, Google en Apple nie dieselfde mate van sekuriteit bied as professionele sisteme nie, soos later bespreek word.

Die volgende onderafdeling bespreek die kommunikasiesisteme van hierdie beheersisteme.

Kommunikasiesisteem

Hierdie afdeling fokus op die bekendste kommunikasiesisteme, maar ander bestaan ook en word byvoorbeeld in Kauranen (2021) en Horyachyy (2017) bespreek. Die kommunikasiesisteme wat hier bespreek word, word algemeen gesien as die markleiers (Ammar et al., 2018), en Hikvision (2021b) verskaf byvoorbeeld ook 'n kort vergelyking van hierdie sisteme.

Die meeste slimhuissisteme kommunikeer met behulp van radiogolwe, waarvan Zigbee en Z-Wave die algemeenste is. Zigbee is gebaseer op die 802.15.4-protokol van die Instituut vir Elektriese en Elektroniese Ingenieurs (IEEE) (Horyachyy, 2017; Kuzminykh et al., 2017; Robles en Kim, 2010). Dit is 'n draadlose netwerktegnologie wat meesal deur middel van 'n frekwensie van 2,4 GHz kommunikeer (maar ook op 868 MHz en 915 MHz) met toepassings wat relatief ongereelde data-uitruilings teen lae datatempo›s oor 'n beperkte gebied en binne 'n 100 m-radius benodig, byvoorbeeld binne 'n huis of gebou (Danbatta en Varol, 2019; Hikvision, 2021b; Horyachyy, 2017; Kauranen, 2021; Kuzminykh et al., 2017;). Zigbee se reikafstand is in Kuzminykh et al. (2017) getoets en die outeurs het bevind dat Zigbee slegs tot op 60 m in ooptes en 25 m binnenshuis effektief is. Zigbee-toestelle herlei egter die seine (Horyachyy, 2017; Kauranen, 2021), wat tot gevolg het dat 'n Zigbee-toestel 25 m van die naaste Zigbee-toestel moet wees, nie noodwendig 25 m van die spilpunt nie. Zigbee sluit ook sekuriteit in deur middel van Advanced Encryption Standard-enkripsie (AES-enkripsie) (128-greep) (Horyachyy, 2017; Kauranen, 2021). Toestelle wat met Zigbee kommunikeer, het gewoonlik 'n batteryleeftyd van ongeveer twee jaar (Hikvision, 2021b). Zigbee word byvoorbeeld deur Philips Hue (Hilbolling et al., 2021; Horyachyy, 2017) en IKEA Trådfri (Kauranen, 2021) gebruik.

Z-Wave kommunikeer met 'n frekwensie van 900 MHz en het 'n reikwydte van ongeveer 30 m (Danbatta en Varol, 2019; Horyachyy, 2017; Kauranen, 2021), alhoewel Hikvision (2021b) die reikwydte van die vyfde generasie van Z-Wave as 150 m aandui. Soos Zigbee gebruik Z-Wave ook toestelle as herleiers en laat ook AES-inkripsie toe (Kauranen, 2021). Toestelle wat met Z-Wave kommunikeer, het 'n gemiddelde batteryleeftyd van twee jaar (Hikvision, 2021b).

Wi-Fi is gebaseer op die IEEE 802.11-standaard en werk in frekwensies van 2,4 GHz en 5 GHz (Danbatta en Varol, 2019; Horyachyy, 2017; Kauranen, 2021). Wi-Fi het 'n maksimum reikafstand van 1 000 m (Danbatta en Varol, 2019), maar soos met ander radioprotokolle beperk hindernisse Wi-Fi se reikafstand en Kauranen (2021) stel Wi-Fi se reikwydte as 70 m binnenshuis en 250 m buite, terwyl Hikvision (2021b) Wi-Fi se reikwydte as minder as 100 m stel. Alhoewel Wi-Fi in staat is om meer data te hanteer as Z-Wave en Zigbee, benodig Wi-Fi meer energie, wat die gebruik daarvan vir draadlose sensors beperk (Horyachyy, 2017), en volgens Hikvision (2021b) word Wi-Fi-toestelle gewoonlik nie met batterye gebruik nie. Slimhuiskameras gebruik egter gereeld Wi-Fi, omdat Wi-Fi meer data as Zigbee of Z-Wave kan hanteer. Kauranen (2021) bespreek die verskillende weergawes van Wi-Fi.

Bluetooth is kortafstand- draadlose tegnologie gebaseer op die IEEE 802.15.1-standaard en het volgens Horyachyy (2017) 'n reikwydte van 10 m, alhoewel Kauranen (2021) skryf dat Bluetooth se reikafstand 50 m binnenshuis en 100 m buitenshuis is, wat tot 1 000 m verleng kan word. Hikvision (2021b) stel ook Bluetooth se reikwydte as 100 m. Bluetooth funksioneer ook op 2,4 GHz en laat AES-128-greepenkripsie toe (Kauranen, 2021; Stute et al., 2021). Die batteryleeftyd van Bluetooth-toestelle is ongeveer een jaar (Hikvision, 2021b).

Daar bestaan groot kommer oor die veiligheid van toestelle wat deur middel van radioverbindings met mekaar verbind is (Abu Waraga et al., 2020; Bugeja, 2021; Doan et al., 2018; Maras, 2015; Meng et al., 2018; Stute et al., 2021). Radioprotokolle soos Z-Wave en Zigbee se kwesbaarheid ten opsigte van kuberkrakers is reeds uitgewys (Badenhop et al., 2017; Yassein et al., 2018), sowel as gebreke in Bluetooth se sekuriteit (Antonioli et al., 2019) en sekuriteitsgebreke in slimfoontoepassings (Fernandes et al., 2016). Krakers kan in beginsel deur slimhuistoestelle inluister of selfs direkte beheer oorneem (Fernandes et al.,

2016; Meng et al., 2018), wat byvoorbeeld sou kon beteken dat kuberkrakers persoonlike gesprekke sou kon opneem, kameras aktiveer, deure oopsluit of selfs brande stig. Daar is egter deurlopende ontwikkelings om sekuriteit te verbeter. 'n Verdere probleem met hierdie toestelle is dat baie verskillende toestelle op dieselfde frekwensie funksioneer, wat tot gevolg het dat radioseine om dieselfde golflengte meeding en soms onderbreek word (Hikvision, 2021a).

Ajax het hierdie sekuriteitsgebreke hanteer deur hulle eie radioprotokol te ontwikkel, naamlik die Jeweller-radioprotokol (Anoniem, 2019a; Mokrenko en Partola, 2019). Die sisteem kontroleer sy werking elke 12 sekondes, pas die radiofrekwensie aan indien dit ontwrig word ("frequency hopping"), en wanneer die verbindings verbreek word, word 'n alarm outomaties geaktiveer (Anoniem, 2019a). Die spilpunt kan met sensors so ver weg as 2 000 m kommunikeer en die batteryleeftyd van sensors is ongeveer sewe jaar (Hikvision, 2021b).

Hikvision se AX Pro-sisteem gebruik ook hulle eie radioprotokol, Tri-X (Cam-X hanteer foto- en videomateriaal) (Anoniem, 2020; Hikvision, 2020; 2021a). Soos met Jeweller verander die sisteem ook van frekwensie om te verseker dat radioseine nie onderbreek word nie, en indien dit wel gebeur, word die gebruiker onmiddellik daarvan in kennis gestel (Hikvision, 2021a; 2021b). Tri-X se reikwydte is ook tot op 2 000 m en die batteryleeftyd van sensors is ses jaar (Hikvision, 2021b). Tri-X gebruik Hikvision se eie enkripsie, wat op AES gebaseer is (Hikvision, 2021a; 2021b).

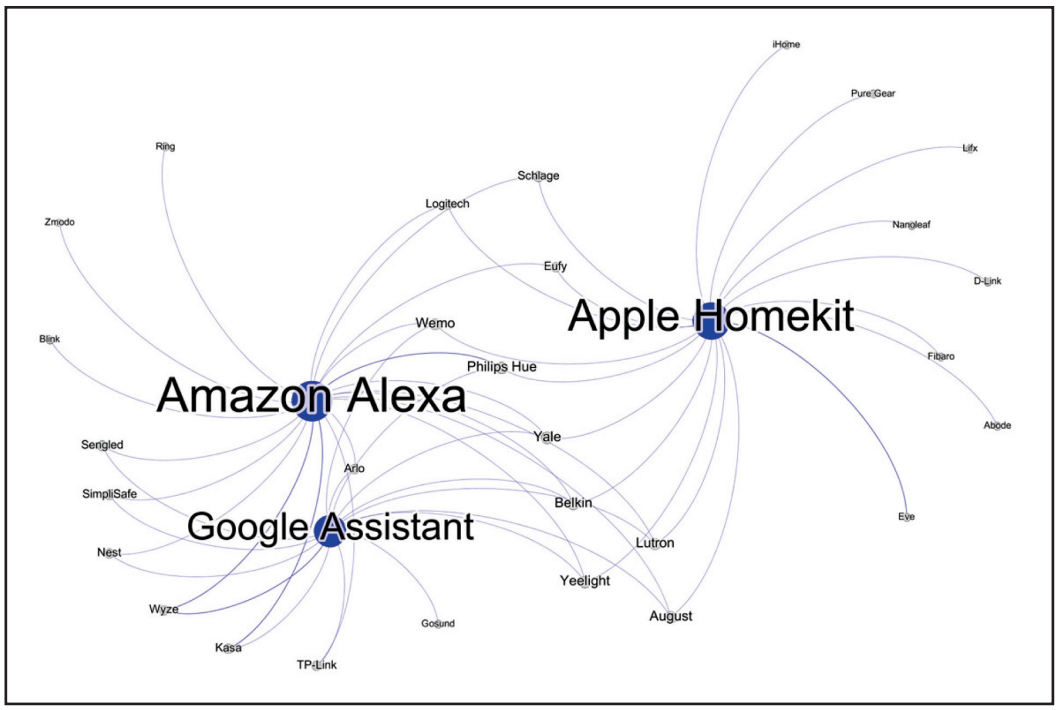
Die volgende afdeling bespreek die algemeenste soorte sensors wat binne bostaande sisteme geïntegreer kan word.

Fisiese komponente

Daar bestaan só 'n groot verskeidenheid fisiese komponente wat binne slimhuis-beheersisteme geïntegreer kan word dat 'n sistematiese oorsig nie binne 'n enkele studie voltrek kan word nie. Iyer en Basole (2016) stel voor dat slimhuis-beheersisteme en toestelle as 'n netwerk gevisualiseer kan word ten einde 'n beter begrip van die veld te bekom, en hierdie artikel volg hulle voorbeeld. Hiervoor word voorstelle gebruik wat deur verskeie outeurs ten opsigte van toestelle binne die Amazon Alexa/Echo, Google Assistant/Nest en Apple Homekit/Siri-ekosisteme gemaak word (Bizzaco en McGrath, 2021; Bizzaco en Rawes, 2021; Bradford, 2021; Cericola, 2020; Chase, 2021; Dunn, 2020; Gebhart en Price, 2021; Hayes en De Looper, 2021; Hill, 2021a; 2021b; Price, 2021; Priest en Wollerton, 2021).

Figuur 2 vertoon die netwerk van verbindings tussen beheersisteme (in blou) en vervaardigers (in grys) van produkte wat deur hierdie outeurs voorgestel word. Alhoewel hierdie netwerk nie 'n verteenwoordigende oorsig oor die veld verskaf nie, gee dit wel 'n aanduiding van watter maatskappye tans belangrike rolspelers in hierdie mark is. Dit is ook opmerklik dat Amazon Alexa en Google Assistant nader aan mekaar geposisioneer is, wat die gevolg is daarvan dat meer vervaardigers se toestelle met albei sisteme versoenbaar is, terwyl Apple Homekit verbintenisse met sy eie stel vervaardigers het. Sommige vervaardigers, soos Philips Hue, August, Yale en Lutron, word deur bogenoemde outeurs met al drie beheersisteme verbind.

Die volgende onderafdelings bespreek toestelle in meer besonderhede.



FIGUUR 2: Belangrike rolspelers in die slimhuismark (2021)

Beligting

Beligting is 'n belangrike komponent van 'n veiligheidsisteem omdat dit eerstens indringers sigbaar maak, maar ook omdat dit videomonitering verbeter (Department of Homeland Security, 2019). Verder vind die meeste huisrooftogte en plaasaanvalle in Suid-Afrika in die aand en in die nag plaas (Hornschuh, 2007; Lancaster, 2013; Zinn, 2008), wat beteken dat goeie beligting in 'n Suid-Afrikaanse veiligheidsisteem 'n prioriteit behoort te wees.

Philips Hue is in 2012 bekendgestel en is die gewildste slimhuis-ligtoepassing (Hilbolling et al., 2019; 2021; Weaver et al., 2020), maar IKEA, LIFX, Eufy, Yeelight en Hive het ook 'n groot deel van die mark oorgeneem. Philips Hue laat die gebruiker toe om beheer oor beligting uit te oefen, wat insluit die helderheid van ligte, hulle kleur, watter ligte tegelykertyd aan- en afskakel, ensovoorts (Porter et al., 2019). Die sisteem sluit ook binne- en buite-bewegingsensors met ingeboude ligsensors in, wat beteken dat ligte só gestel kan word dat dit outomaties met sononder aangaan, of spesifieke ligte kan aan- of afskakel wanneer beweging geregistreer word (Brown, 2019; Mead, 2020). Philips Hue vervaardig ook slimmuurproppe, wat gewone ligte by die sisteem kan integreer. Hierdie sisteem is versoenbaar met Apple Siri, Google Assistant en Amazon Alexa (Hilbolling et al., 2019; Porter et al., 2019), wat beteken dat dit ook deur middel van 'n stembevel geaktiveer kan word (Mead, 2020). Verder laat die sisteem die gebruiker toe om sy ligging te gebruik om roetines te aktiveer, byvoorbeeld om alle ligte outomaties aan te skakel wanneer die gebruiker tuiskom (Porter et al., 2019).

Soos met ander slimhuissisteme is die sekuriteit van die netwerk nie altyd voldoende nie en gebreke in Philips Hue se sekuriteit is reeds uitgewys (Kafle et al., 2021; Notra et al., 2014; Ronen en Shamir, 2016). In die geval van 'n beligtingsisteem beteken 'n kuberaanval op Philips Hue egter slegs dat krakers ligte aan en af kan skakel, en boonop moes Ronen en Shamir (2016) fisies naby die perseel wees om die sisteem te penetreer.

Indringeropsporingsisteem

Bewegingsensors

Passiewe infrarooisensors (PIR-sensors) is een van die algemeenste tipes sensors vir die opsporing van beweging. Hierdie sensors registreer die hittespoor van indringers deur die sensor se infrarooi-ontvangs met normale agtergrond-infrarooivlakke te vergelyk (Department of Homeland Security, 2019). PIR-sensors veroorsaak gereeld vals alarms wanneer ander objekte, byvoorbeeld troeteldiere, se hitte geregistreer word, of wanneer gereflekteerde lig op die sensor skyn, maar dit is baie moeilik vir 'n indringer om PIR-sensors te omseil (Department of Homeland Security, 2019).

Omdat dit so 'n bekende tegnologie is, vervaardig die meeste slimhuismaatskappye PIR-sensors. Sommige maatskappye, soos Ajax, Eve, Hikvision, Philips Hue en Yale, vervaardig beide binnens- en buitenshuise PIR-sensors, terwyl ander maatskappye slegs binnenshuise sensors vervaardig. Fibaro vervaardig 'n sensor wat binne en buite gebruik kan word en boonop die temperatuur ook meet, terwyl Philips Hue se binne- en buitesensors ook lig en temperatuur meet. Die grootste waarde van hierdie sensors lê daarin dat hulle outomatiserings binne Amazon Echo, Google Nest of Apple Homekit kan begin, byvoorbeeld om 'n lig aan te skakel wanneer beweging geregistreer word, of andersins om 'n kennisgewing na 'n gebruiker se slimfoon te stuur of 'n alarm te aktiveer.

Sommige maatskappye, soos Ajax, Hikvision en Yale, vervaardig PIR-sensors wat ook foto's neem om alarms visueel te verifieer (Anoniem, 2020; Hikvision, 2020). Sulke sensors werk soortgelyk aan wildkameras ("trail cameras") en kan ook vals alarms verminder deur visuele identifikasie te bemiddel. Hierdie maatskappye se gewone buite-PIR-sensors is ook ontwerp om nie vals alarms te registreer wanneer troeteldiere binne die sensor se opsporingsruimte beweeg nie. Nie een van hierdie PIR-sensors van Ajax, Hikvision en Yale kan egter binne Amazon, Google of Apple se sisteme geïntegreer word nie.

Deur- en vensterkontakte

Deur- en vensterkontakte kan meganies, magneties of deur middel van 'n gebalanseerde magnetiese skakelaar werk (Department of Homeland Security, 2019). Dit is ook 'n bekende tegnologie en word onder andere deur Ajax, Eufy, Eve, Fibaro, Hikvision, Wyze en Yale vervaardig. Hierdie sensors maak dit verder moontlik om outomatiserings te begin, kennisgewings uit te stuur of 'n alarm te registreer. 'n Groot nadeel van hierdie sensors is egter dat dit slegs bruikbaar is vir outomatiserings en wanneer die eienaar nie tuis is nie; in die geval van 'n huisroof skep hierdie sensors te min tyd om te reageer.

Glasbreeksensors

Daar bestaan drie tipes glasbreeksensors: akoestiese sensors (wat luister na 'n akoestiese klankgolf wat ooreenstem met die frekwensie van gebreekte glas), skoksensors (wat die skokgolf registreer as glas gebreek word), en sensors met dubbele tegnologie (akoestiese sensors gekombineer met skokvibrasies) (Department of Homeland Security, 2019). Maatskappye wat hierdie soort sensors vervaardig, sluit in Ajax, Hikvision en SimpliSafe. Amazon Alexa kan ook die klank van glas wat breek, herken en daarvolgens 'n alarm registreer, maar alhoewel Apple se iOS soortgelyke funksionaliteit het, kan dit nie tans binne 'n sekuriteitsisteem geïntegreer word nie, omdat Apple nie toelaat dat die kennisgewing tussen toestelle gestuur word nie (Carman, 2020). Soos die geval is met deur- en vensterkontakte, verskaf hierdie sensors nie vroeë waarskuwing nie, maar dit kan benut word wanneer die eienaar nie tuis is nie.

Toegangsbeheersisteem

'n Toegangsbeheersisteem kan elektroniese slotte, kaartlesers en biometriese lesers bevat (Department of Homeland Security, 2019). Toegangsbeheersisteme laat mense toe om gemagtigde gebruikers by die sisteem te voeg, toegangstoestemmings vir gebruikers in te stel en gebeure en alarms te monitor. Hierdie funksionaliteit is ingebou in Amazon Echo, Google Nest en Apple Homekit, sowel as in Ajax en Hikvision AX PRO. Die huidige onderafdeling bespreek die fisiese komponente wat toegangsbeheer bemiddel.

Kodegebaseerde toegangsmeganismes

Kodegebaseerde toestelle soos sleutelborde werk volgens die beginsel dat 'n persoon 'n kode of PIN ontvang het om in die toestel in te voer wat die egtheid van die ingevoerde kode sal verifieer (Department of Homeland Security, 2019). Dit is ook 'n bekende tegnologie wat binne die meeste sisteme beskikbaar is, byvoorbeeld Hikvision AX Pro, Ajax, Eufy, Yale en SimpliSafe.

Biometriese toegangsmeganismes

Biometriese toestelle vergelyk 'n spesifieke biologiese eienskap met 'n gestoorde templaat. Vingerafdrukke, gesigspatrone, handmeetkunde en irisskandering is die oorheersende biometriese tegnieke wat gebruik word (Department of Homeland Security, 2019). Hierdie tegnologie het oor die afgelope paar jaar beduidend goedkoper geword en toestelle wat biometriese herkenning gebruik, word tans deur maatskappye soos Dioche, Eufy, Harfol, Samsung, Sifely en Ultraloq vervaardig.

Elektroniese slotte

Elektroniese slotte laat die gebruiker toe om deure met sy foon oop en toe te sluit, wat beteken dat die gebruiker ook vir gaste kan oopsluit wanneer hy nie tuis is nie. Verder maak outomatiserings dit moontlik om deure outomaties te sluit, byvoorbeeld 30 sekondes nadat 'n deur oopgesluit is, of wanneer die gebruiker gaan slaap. Maatskappye wat slimslotte vervaardig, is onder andere August, Eufy, Schlage, SimpliSafe, Ultraloq, Wyze en Yale. In Suid-Afrika vervaardig Trellidor ook roldeure wat by 'n slimhuissisteem geïntegreer kan word en skep daardeur die geleentheid om bykomende sekuriteit, byvoorbeeld 'n veiligheidsone, by die slimhuissisteem te betrek (Trellidor, 2020).

Kamerasisteem

Daar is 'n groot verskeidenheid kameras op die mark en kamerategnologie het onlangs tot só 'n mate bekostigbaar geword dat dit binne die meeste slimhuisgebruikers se bereik is. Kameras kan bedraad of draadloos wees, met of sonder nagsig, termies of net met nagsig toegerus (wat beelde met infrarooilig verlig), en met of sonder beeldherkenning deur kunsmatige intelligensie. Die verskillende soorte kameras word in Department of Homeland Security (2019) bespreek.

Maatskappye wat kameras vir slimhuise vervaardig, is onder andere Arlo, Eufy, Eve, Google Nest, Hikvision, Logitech, Ring, SimpliSafe, Wyze en Yale. Hierdie kameras se vermoëns en versoenbaarheid verskil, maar breedweg laat slimhuiskameras die gebruiker toe om kameras só op te stel dat die gebruiker kennisgewings kan ontvang wanneer 'n spesifieke beweging, byvoorbeeld 'n persoon of 'n motor, opgemerk word. Die gebruiker kan ook gewoonlik kameras deur 'n slimfoontoepassing soos Apple Homekit monitor.

Die VSA se Department of Homeland Security (2019) beveel nie aan dat kameras as die primêre indringeropsporingsisteem gebruik word nie omdat tradisionele indringeropsporingsensors oor die algemeen beter as video-ontleding vaar ten opsigte van die waarskynlikheid van opsporing, alarmfrekwensie, integrasie met alarmmoniteringsisteme en koste. Nietemin kan kameras met vrug aangewend word om alarms te verifieer en ook andersins die perseel te monitor.

Die volgende afdeling bespreek hoe fisiese komponente binne 'n beheersisteem geïntegreer kan word.

'n Slimhuis-veiligheidsisteem in Apple Homekit

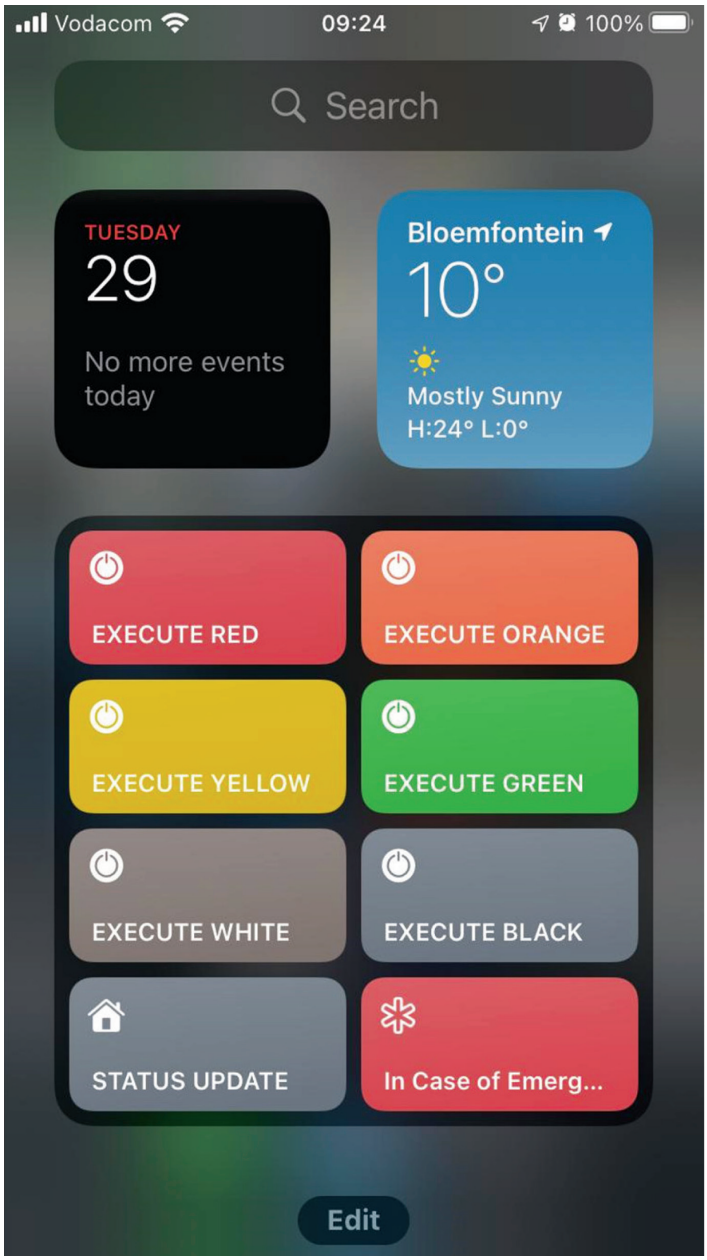
Teen die agtergrond van die voorafgaande bespreking is dit moeilik om 'n aanbeveling ten opsigte van slimhuisbeheersisteme te maak. Vir Apple-gebruikers is Homekit dalk ideaal: Apple is strenger met privaatheidsregulasies as Amazon en Google (Chase, 2021; Yoffie et al., 2018), en die opstel van toestelle en outomatiserings is meer intuïtief as ander slimhuissisteme (Chase, 2021; Fifield, 2020; Hearn, 2020). Google Assistant en Amazon Alexa se stemherkenning is egter akkurater as Apple se Siri (Chase, 2021; Yoffie et al., 2018), en daar is ook baie meer toestelle wat binne hierdie sisteme geïntegreer kan word as met Apple Homekit. Die sekuriteitsgebreke in al drie hierdie sisteme, tesame met die kort reikafstande van die radioprotokolle wat gebruik word en die gevaar dat seine onderbreek kan word, noop 'n mens egter om ernstig te besin oor of hierdie sisteme tans betroubaar genoeg is om in 'n Suid-Afrikaanse opset op te steun, waar misdaad nie slegs die verlies aan eiendom meebring nie, maar ook van lewens. Wanneer 'n betroubare en veilige sekuriteitsisteem verlang word, is doelgerigte sisteme soos dié van Ajax of Hikvision geskikter, alhoewel hierdie sisteme nie met die markleiers se sisteme geïntegreer kan word nie.

Gebreke in slimhuissisteme beteken egter nie dat Apple, Google en Amazon nie ook in 'n aanvullende en voorkomende rol benut kan word nie. Ajax en Hikvision vervaardig byvoorbeeld nie beligtingsisteme of elektroniese slotte nie, terwyl hierdie bekende toepassings binne Amazon, Google en Apple beskikbaar is. Slimslotte kan byvoorbeeld gebruik word om te verseker dat deure gesluit word, terwyl beligtingsisteme aangewend kan word om die indruk te skep dat die eienaar tuis is.

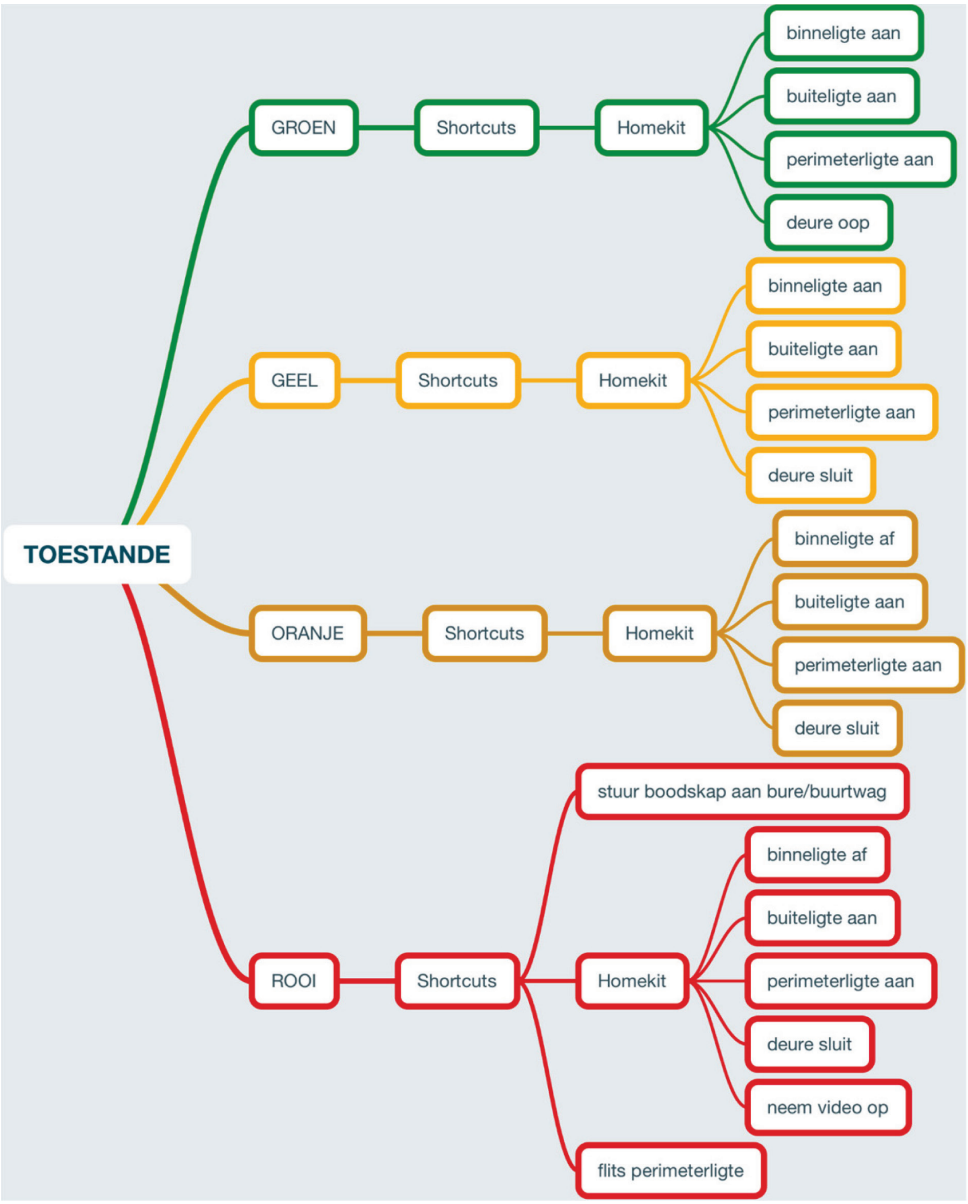
Omdat Apple se sisteem veiliger is as dié van Google en Amazon en deur Shortcuts verryk kan word, is Homekit in die huidige studie gebruik om 'n voorbeeld van 'n aanvullende en gebruikersvriendelike veiligheidsisteem te skep. Hiervoor is 'n iPad en iPhone (enige model is geskik) met iOS 14.6 gebruik. Die iPad funksioneer as spilpunt, omdat Homekit vereis dat 'n iPad, Apple TV of HomePod as spilpunt gebruik moet word (Apple, 2021). Outomatiserings word deur middel van Shortcuts geskep en kan vanaf die Today-blad op 'n iPad of iPhone geaktiveer word. Die Today-blad kan in figuur 3 gesien word. Toestande is in Engels opgestel omdat Apple Siri nie Afrikaans magtig is nie.

Toestande is vir verskillende vlakke van waaksaamheid geskep, soos in figuur 3 gesien kan word. Vier toestande is in Shortcuts geskep: groen, geel, oranje en rooi. Daar is ook 'n swart en wit toestand geskep, wat onderskeidelik alle ligte aan- of afskakel, maar omdat hierdie eenvoudige toestande is, word dit nie hieronder aangedui nie. Die kortpad *Status update* beheer die sisteem en verskaf terugvoer oor werkverrigting, terwyl *In case of emergency* 'n paniekknoppie verteenwoordig wat ook weg van die perseel gebruik kan word en as verstek by Shortcuts ingesluit is. Ligte is in verskeie vertrekke gegroepeer, maar ter wille van eenvoud word slegs die woonarea hieronder in tonele benoem. Daar is ook buiteligte en ligte op die heining gespesifiseer, wat beide deur middel van 'n Philips Hue-slimmuurprop beheer word.

Figuur 4 dui die toestande aan. Let daarop dat bewegingsensors ten alle tye aan is en daarom nie in die diagram aangetoon word nie.



FIGUUR 3: Die Today-blad op 'n iOS-toestel



FIGUUR 4: Die toestande wat in Apple Shortcuts en Homekit geskep is

Wanneer die groen toestand geaktiveer word, skakel Homekit alle ligte in die woonkamer, buite die huis en op die heining aan, maar die deure is oopgesluit. Dit sal tipies die toneel wees kort ná sonsondergang en dit kan outomaties ná sononder deur middel van Shortcuts geaktiveer word. Daar kan ook gespesifiseer word of die outomatisering elke dag moet aktiveer of net sommige dae, en of die toestand moet aktiveer wanneer mense tuis is of nie. Die toestand kan ook deur middel van 'n stembevel, vanuit 'n iOS-toestel se Today-blad, of vanuit Homekit se paneelbord geaktiveer word, en die toneel kan ook outomaties geaktiveer word indien die inwoners ná donker tuis kom.

Wanneer die geel toestand geaktiveer word, word alle buiteligte en die woonvertrek se ligte aangeskakel, maar die deure sluit ook. Hierdie toneel kan outomaties op 'n sekere tyd deur middel van Shortcuts geaktiveer word, maar soos met ander tonele kan dit ook deur middel van 'n stembevel vanuit Homekit se paneelbord of vanuit 'n iOS-toestel se Today-blad geaktiveer word.

Wanneer die oranje toestand geaktiveer word, word alle ligte binnenshuis afgeskakel, alle ligte buitenshuis sowel as op die heining word aangeskakel, en deure word gesluit. Hierdie toestand is die tipiese toestand wanneer die eienaar gaan slaap, maar kan ook gebruik word wanneer die eienaar vroeër in die aand iets verdags opmerk, of wanneer die eienaar saans die perseel verlaat.

Die rooi toestand funksioneer soos 'n paniekknoppie. Wanneer hierdie toestand vanuit die Today-blad op 'n iOS-toestel geaktiveer word, word daar met behulp van Shortcuts se ingeboude *In case of emergency*-kortpad eerstens 'n boodskap aan die bure en die leier van die buurtwag

gestuur, met die gebruiker se ligging, waarna alle ligte binne afgeskakel word en alle ligte buite, insluitend op die heining, aangeskakel word, deure word gesluit en video-opnames begin. Deur middel van Shortcuts word ligte op die heining ook geflits sodat indringers kan kennis neem daarvan dat hulle opgemerk is, en vir bure om te sien dat daar 'n noodgeval is. Die toestand funksioneer soos volg:

```
Run In case of emergency
    GET Current location
    SEND message [Daar is 'n noodgeval by my. Kom
    help dringend! Ek is by LOCATION] to [Buurman,
    Buurtwag]
SET Code Red
    Turn on Hue smart plug exterior
    Turn off Living room
        Turn off Lamp1
        Turn off Lamp2
        Turn off Main light
    Turn on Hue smart plug perimeter
    Lock doors
REPEAT 20 times
    SET Hue smart plug perimeter ON
    WAIT 1 second
    SET Hue smart plug perimeter OFF
    END REPEAT
SET Code Red
Turn off never
```

Die voordeel daarvan om toestande te skep en dan daardie toestande deur outomatiserings te aktiveer, is dat toestande ook deur sensors geaktiveer kan word. Wanneer 'n bewegingsensor byvoorbeeld beweging registreer, kan die toestand geel geaktiveer word, wat ligte binne die huis aanskakel en kontroleer dat ligte buite die huis aan is. Die toestand rooi sou ook geaktiveer kon word wanneer 'n deurkontak registreer dat 'n deur oopgemaak is, wat outomaties bure in kennis sal stel dat daar 'n bedreiging is deur ligte te flits. Wanneer die toestand rooi deur Homekit geaktiveer word, kan 'n boodskap egter as gevolg van die beperkte integrasie tussen Shortcuts en Homekit nie aan die bure gestuur word nie.

Slot

Slimhuistegnologie beskik oor groot potensiaal om mense se veiligheid te verbeter. Hierdie tegnologie het oor die afgelope paar jaar in gewildheid toegeneem, wat beteken dat 'n groot hoeveelheid maatskappye toestelle begin vervaardig het om die huis te monitor. Die tendens is dat sisteme beter met mekaar integreer, die sekuriteit van toestelle word deurgaans verbeter, en beheersisteme word slimmer namate kunsmatige intelligensie tot 'n groter mate by hierdie sisteme geïntegreer word. Die huidige studie het sommige van hierdie toestelle, kommunikasiesisteme en beheersisteme ondersoek, sowel as hulle vermoëns en gebreke. Laastens is 'n voorbeeld verskaf van hoe 'n slim-huis in Apple Homekit opgestel sou kon word om veiligheid outomaties te verbeter.

Die slimhuismark is 'n baie dinamiese veld en tegnologiese verbeterings vind gereeld plaas. Die huiseienaar wat van slimhuistegnologie gebruik wil maak, sal deurlopend op hoogte moet bly van tegnologiese veranderinge en ook sy sisteem aanpas.

Bronnelys

Abu Waraga, O., Bettayeb, M., Nasir, Q., Abu Talib, M. 2020. Design and implementation of automated IoT security testbed. Computers & Security 88, 101648. https://doi.org/10.1016/j.cose.2019.101648.

Adam, F.M. 2021. Drivers of violent property crime in South Africa: A system dynamics model focussing on education and income inequality. Master's-degree thesis. Stellenbosch University.

Ajax. 2021a. How to create and configure a scenario in the Ajax security system. https://support.ajax.systems/en/manuals/scenarios/ (geraadpleeg op 4 Junie 2021).

Ajax. 2021b. The history of Ajax Systems. https://newsroom.ajax.systems/en/history/ (geraadpleeg op 21 Mei 2021).

Albǵstroiu, I., Enache, C., Cepoi, A., Istrate, A., Andrei, T.L. 2021. Adopting IoT-based solutions for smart homes. The perspective of the Romanian users. Advances in Entomology 23(57), 325-341.

Ammar, M., Russello, G., Crispo, B. 2018. Internet of things: A survey on the security of IoT frameworks. Journal of Information Security and Applications 38, 8-27. https://doi.org/10.1016/j.jisa.2017.11.002.

Anderson, M.E. 2018. Technical trade-offs of IoT platforms, in Dudzik, M.C. en Ricklin, J.C. (reds.). Autonomous systems: sensors, vehicles, security, and the internet of everything, 44. https://doi.org/10.1117/12.2302615.

Anoniem. 2019a. Effective intruder detection: more important than ever. Hi-Tech Security Solutions 25(4), 66.

Anoniem. 2019b. Not just intruder detection systems. High-Tech Security Solutions, 25(9), 39.

Anoniem. 2020. AX PRO wireless alarm solutions. Hi-tech Security Solutions 26(8), 31.

Antonioli, D., Tippenhauer, N.O., Rasmussen, K. 2019. The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation of Bluetooth BR/EDR. In: Proceedings of the 28th USENIX Conference on Security Symposium. 28th USENIX Conference on Security Symposium, USA: USENIX Association (SEC'19), 1047-1061.

Apple. 2021. Your home at your command. https://www.apple.com/ios/home/ (geraadpleeg op 4 Junie 2021).

Badenhop, C.W., Graham, S.R., Ramsey, B.W., Mullins, B.E., Mailloux, L.O. 2017. The Z-Wave routing protocol and its security implications. Computers & Security 68, 112-129. https://doi.org/10.1016/j.cose.2017.04.004.

Bizzaco, M., McGrath, J. 2021. The best Alexa-enabled devices for 2021. https://www.digitaltrends.com/home/best-alexa-enabled-devices/ (geraadpleeg op 11 Junie 2021).

Bizzaco, M., Rawes, E. 2021. The best Apple HomeKit-compatible devices for 2021. https://www.digitaltrends.com/home/best-apple-homekit-enabled-devices/ (geraadpleeg op 11 Junie 2021).

Bradford, A. 2021. The best Google assistant-compatible devices for 2021. https://www.digitaltrends.com/home/best-google-home-compatible-devices/ (geraadpleeg op 11 Junie 2021).

Brown, M. 2019. Philips Hue outdoor motion sensor review: A must-have accessory for Hue smart lighting owners. https://www.techhive.com/article/3346228/philips-hue-outdoor-motion-sensor-review.html (geraadpleeg op 27 Mei 2021).

Bugeja, J. 2021. On privacy and security in smart connected homes. Doctoral dissertation. Malmö University.

Bu, L., Xiong, W., Liang, C.J.M., et al. 2018. Systematically ensuring the confidence of real-time home automation IoT Systems. ACM Transactions on Cyber-Physical Systems, 2(3), 1-23. https://doi.org/10.1145/3185501.

Capodieci, A., Budner, P., Eirich, J., Gloor, P., Mainetti, L. 2018. Dynamically adapting the environment for elderly people through smartwatch-based mood detection. In: Grippa, F., Leitão, J., Gluesing, J., Riopelle, K. en Gloor, P. (reds.). Collaborative Innovation Networks. Cham: Springer International Publishing (Studies on entrepreneurship, structural change and industrial dynamics), 65-73. https://doi.org/10.1007/978-3-319-74295-3_6.

Carman, A. 2020. New iOS 14 feature lets the iPhone alert you if it hears sounds like a doorbell or fire alarm. https://www.theverge.com/21300261/ios-14-update-smoke-alarm-sound-detection-accessbility (geraadpleeg op 4 Junie 2021).

Cericola, R. 2020. The best Alexa-compatible smart-home devices for Amazon Echo. https://www.nytimes.com/wirecutter/reviews/best-alexa-compatible-smart-home-devices-for-amazon-echo/ (geraadpleeg op 11 Junie 2021).

Chase, J. 2021. How to build an Apple-based smart home system with the best homekit devices. https://www.nytimes.com/wirecutter/reviews/best-homekit-devices/ (geraadpleeg op 11 Junie 2021).

Clark, M., Dutta, P. 2015. The haunted house: networking smart homes to enable casual long-distance social interactions. In: Proceedings of the 2015 International Workshop on Internet of Things towards Applications. SenSys ‹15: The 13th ACM Conference on Embedded Network Sensor Systems, New York, NY, USA: ACM, 23-28. https://doi.org/10.1145/2820975.2820976.

Danbatta, S., Varol, A. 2019. Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth wireless technologies used in home automation. In: 2019 7th International Symposium on Digital Forensics and Security (ISDFS). 2019 7th International Symposium on Digital Forensics and Security (ISDFS), IEEE, 1-5. https://doi.org/10.1109/ISDFS.2019.8757472.

Davis, K., Jun, H., Feijs, L., Owusu, E. 2015. Social Hue: A subtle awareness system for connecting the elderly and their caregivers. In: 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops). 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), IEEE, 178-183. https://doi.org/10.1109/PERCOMW.2015.7134015.

Demiris, G., Hensel, B.K. 2008. Technologies for an aging society: a systematic review of ‘smart home’ applications. Yearbook of Medical Informatics, 33-40. https://doi.org/10.1055/s-0038-1638580.

Department of Homeland Security. 2019. Unified facilities criteria (UFC) Electronic Security Systems.

De Silva, L.C., Morikawa, C., Petra, I.M. 2012. State of the art of smart homes. Engineering Applications of Artificial Intelligence, 25(7), 1313-1321. https://doi.org/10.1016/j.engappai.2012.05.002.

Doan, T.T., Safavi-Naini, R., Li, S., et al. 2018. Towards a resilient smart home. In Proceedings of the 2018 Workshop on IoT Security and Privacy - IoT S&P ‘18. The 2018 Workshop, New York, New York, USA: ACM Press, 15-21. https://doi.org/10.1145/3229565.3229570.

Dunn, T. 2020. The best Google Assistant-compatible smart-home devices for Google Home. https://www.nytimes.com/wirecutter/reviews/best-google-assistant-compatible-smart-home-devices-for-google-home/ (geraadpleeg op 11 Junie 2021).

Einarsson, A.F., Patreksson, P., Hamdaqa, M., Hamou-Lhadj, A. 2017. SmartHomeML: Towards a domain-specific modeling language for creating smart home applications. In: 2017 IEEE International Congress on Internet of Things (ICIOT). 2017 IEEE International Congress on Internet of Things (ICIOT), IEEE, 82-88. https://doi.org/10.1109/IEEE.ICIOT.2017.35.

Fernandes, E., Jung, J., Prakash, A., 2016. Security analysis of emerging smart home applications. In: 2016 IEEE Symposium on Security and Privacy (SP). 2016 IEEE Symposium on Security and Privacy (SP), IEEE, 636-654. https://doi.org/10.1109/SP.2016.44.

Fifield, N. 2020. Apple HomeKit application and cost breakdown. Undergraduate thesis. California Polytechnic State University.

Fogli, D., Peroni, M., Stefini, C. 2017. ImAtHome: Making trigger-action programming easy and fun. Journal of Visual Languages & Computing, 42, 60-75. https://doi.org/10.1016/j.jvlc.2017.08.003.

Gebhart, A., Price, M. 2021. Best Nest and Google Assistant devices of 2021. https://www.cnet.com/home/smart-home/best-google-assistant-nest-devices/ (geraadpleeg op 18 Junie 2021).

Hayes, T., De Looper, C. 2021. The 12 best HomeKit devices of 2021. https://www.businessinsider.com/best-homekit-devices?IR=T (geraadpleeg op 11 Junie 2021).

Hearn, P. 2020. Alexa vs. Google Assistant vs. HomeKit: Which smart home platform to choose? https://www.digitaltrends.com/home/alexa-vs-google-assistant-vs-homekit/ (geraadpleeg op 20 Mei 2021).

Hikvision. 2020. Hikvision launches AX PRO for comprehensive wireless alarm solutions. https://www.hikvision.com/en/newsroom/latest-news/2020/hikvision-launches-ax-pro-for-comprehensive-wireless-alarm-solutions/ (geraadpleeg op 3 Junie 2021).

Hikvision. 2021a. AXPRO Wireless Intrusion Alarm System White Paper. https://www.hikvision.com/content/dam/hikvision/en/brochures-download/product-brochures/alarm/hikvision-intrusion-alarm-panel/AXPRO-Wireless-Intrusion-Alarm-System-White-Paper.pdf (geraadpleeg op 29 Junie 2021).

Hikvision. 2021b. The wireless connection between the Hikvision Hub and the detectors is excellent! https://hikvision-alarm-system.eu/en/tri-x-the-wireless-technology-of-hikvision-ax-pro/ (geraadpleeg op 3 Junie 2021).

Hilbolling, S., Berends, H., Deken, F., Tuertscher, P. 2019. Complementors as connectors: managing open innovation around digital product platforms, R and D Management. https://doi.org/10.1111/radm.12371.

Hilbolling, S., Berends, H., Deken, F., Tuertscher, P., 2021. Sustaining complement quality for digital product platforms: A case study of the Philips Hue ecosystem. Journal of Product Innovation Management, 38(1), 21-48. https://doi.org/10.1111/jpim.12555.

Hill, S. 2021a. The 10 best devices of 2021 that work with Amazon Alexa. https://www.businessinsider.com/best-alexa-devices?IR=T (geraadpleeg op 11 Junie, 2021).

Hill, S. 2021b. The 10 best Google Assistant-enabled products of 2021. https://www.businessinsider.com/best-google-assistant-nest-devices?IR=T (geraadpleeg op 11 Junie 2021).

Hornschuh, V. 2007. A victimological investigation of farm attacks with specific reference to farmers’ perceptions of their susceptibility, the consequences of attacks for farmers and the coping strategies applied by them after victimisation. Master’s-degree thesis. UNISA.

Horyachyy, O. 2017. Comparison of wireless communication technologies used in a Smart Home:Analysis of wireless sensor node based on Arduino in home automation scenario. Master’s-degree thesis. Blekinge Institute of Technology.

Hosseini, S.S., Agbossou, K., Kelouwani, S., Cardenas, A. 2017. Non-intrusive load monitoring through home energy management systems: A comprehensive review. Renewable and Sustainable Energy Reviews, 79, 1266-1274. https://doi.org/10.1016/j.rser.2017.05.096.

Hoy, M.B. 2018. Alexa, siri, cortana, and more: an introduction to voice assistants. Medical reference services quarterly, 37(1), 81-88. https://doi.org/10.1080/02763869.2018.1404391.

Iyer, B.R., Basole, R.C., 2016. Visualization to understand ecosystems. Communications of the ACM, 59(11), 27-30. https://doi.org/10.1145/3000610.

Kafle, K., Moran, K., Manandhar, S., Nadkarni, A., Poshyvanyk, D. 2021. Security in centralized data store-based home automation platforms. ACM Transactions on Cyber-Physical Systems, 5(1), 1-27.https://doi.org/10.1145/3418286.

Kauranen, J. 2021. Choosing right wireless network for IoT devices. Master’s-degree thesis. Helsinki Metropolia University of Applied Sciences.

Kinsella, B. 2020. Amazon Smart Speaker market share falls to 53% in 2019 with Google The biggest beneficiary rising to 31%, Sonos Also Moves Up. https://voicebot.ai/2020/04/28/amazon-smart-speaker-market-share-falls-to-53-in-2019-with-google-the-biggest-beneficiary-rising-to-31-sonos-also-moves-up/ (geraadpleeg op 20 Mei 2021).

Kuzminykh, I., Snihurov, A., Carlsson, A. 2017. Testing of communication range in ZigBee technology. In: 2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM). 2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), IEEE, 133-136. https://doi.org/10.1109/CADSM.2017.7916102.

Lancaster, L. 2013. The increase in home robbery has occurred because perpetrators see it as a high-gain low-risk undertaking. https://issafrica.org/iss-today/safe-as-houses-what-do-we-know-about-home-robberies-in-south-africa (geraadpleeg op 3 Junie 2021).

Liu, P., Li, G., Jiang, S., Liu, Y., Leng, M., Zhao, J., Wang, S., Meng, X., Shang, B., Chen, L., Huang, S.H. 2019. The effect of smart homes on older adults with chronic conditions: A systematic review and meta-analysis. Geriatric Nursing, 40(5), 522-530. https://doi.org/10.1016/j.gerinurse.2019.03.016.

Longe, O.M., Myeni, L., Ouahada, K. 2019. Renewable energy solution for electricity access in rural South Africa. In: 2019 IEEE International Smart Cities Conference (ISC2). 2019 IEEE International Smart Cities Conference (ISC2), IEEE, 772-776. https://doi.org/10.1109/ISC246665.2019.9071693.

Ly, N.T., Tscharn, R., Preßler, J., et al. 2016. Smart lighting in dementia care facility. In: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing Adjunct - UbiComp ‹16. The 2016 ACM International Joint Conference, New York, New York, USA: ACM Press, 1636-1639. https://doi.org/10.1145/2968219.2968526.

Maras, M.H. 2015. Internet of Things: security and privacy implications. International Data Privacy Law, 5(2), 99-104. https://doi.org/10.1093/idpl/ipv004.

Marikyan, D., Papagiannidis, S., Alamanos, E. 2019. A systematic review of the smart home literature: A user perspective. Technological Forecasting and Social Change, 138, 139-154. https://doi.org/10.1016/j.techfore.2018.08.015.

Mead, D. 2020. Hue outdoor motion sensor: Review. https://linkdhome.com/articles/hue-outdoor-motion-review (geraadpleeg op 27 Mei 2021).

Meng, Y., Zhang, W., Zhu, H., Shen, X.S. 2018. Securing consumer iot in the smart home: architecture, challenges, and countermeasures. IEEE Wireless Communications, 25(6), 53-59. https://doi.org/10.1109/MWC.2017.1800100.

Mokrenko, P.V., Partola, V.V. 2019. Receiver unit wireless security system. Automation, Measuring and Management, 1(1), 72-79.

Nield, D. 2021. The best smart home systems 2021: Top ecosystems explained. https://www.the-ambient.com/guides/smart-home-ecosystems-152 (geraadpleeg op 20 Mei 2021).

Notra, S., Siddiqi, M., Habibi Gharakheili H., Sivaraman V., Boreli R. 2014. An experimental study of security and privacy risks with emerging household appliances. In: 2014 IEEE Conference on Communications and Network Security. 2014 IEEE Conference on Communications and Network Security (CNS), IEEE, 79-84. https://doi.org/10.1109/CNS.2014.6997469.

Patel, S., Park, H., Bonato, P., Chan, L., Rodgers, M. 2012. A review of wearable sensors and systems with application in rehabilitation. Journal of Neuroengineering and Rehabilitation, 9, 21. https://doi.org/10.1186/1743-0003-9-21.

Peetoom, K.K., Lexis, M.A., Joore, M., Dirksen, C.D., De Witte, L.P. 2015. Literature review on monitoring technologies and their outcomes in independently living elderly people. Disability and rehabilitation. Assistive technology, 10(4), 271-294. https://doi.org/10.3109/17483107.2014.961179.

Porter, J., Hanson, M., Knapp, M. 2019. Philips Hue review. https://www.techradar.com/reviews/gadgets/appliances/philips-hue-1124842/review (geraadpleeg op 4 Junie 2021).

Price, M. 2021. Best Apple HomeKit devices for 2021. https://www.cnet.com/home/smart-home/best-apple-homekit-siri-devices/ (geraadpleeg op 18 Junie 2021).

Priest, D., Wollerton, M. 2021. Best Alexa devices for 2021: Ring, Wyze, August and more. https://www.cnet.com/home/smart-home/best-alexa-devices/ (geraadpleeg op 18 Junie 2021).

Robles, R.J., Kim, T.-H. 2010. A Review on security in smart home development. International Journal of Advanced Science and Technology, 15, 13-22.

Ronen, E., Shamir, A. 2016. Extended functionality attacks on iot devices: the case of smart lights. In: 2016 IEEE European Symposium on Security and Privacy (EuroS&P). 2016 IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, 3-12. https://doi.org/10.1109/EuroSP.2016.13.

Sovacool, B.K., Furszyfer Del Rio, D.D. 2020. Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. Renewable and Sustainable Energy Reviews, 120, 109663. https://doi.org/10.1016/j.rser.2019.109663.

Stanley, J. 2019. The history of Smart Home Technology. https://www.familyhandyman.com/article/the-history-of-smart-home-technology/ (geraadpleeg op 4 Junie 2021).

Stute, M., Heinrich, A., Lorenz, J. en Hollick, M., 2021. Disrupting continuity of Apple›s wireless ecosystem security: new tracking, DoS, and MitM attacks on iOS and macOS through Bluetooth low energy, AWDL, and Wi-Fi. In: 30th USENIX Security Symposium (USENIX Security 21). 30th USENIX Security Symposium (USENIX Security 21), USENIX Association.

Trellidor. 2020. Rollerstyle shutter features that will complete your Smart Home. https://blog.trellidor.co.za/2020/07/rollerstyle-shutter-features-that-will-complete-your-smart-home/ (geraadpleeg op 4 Junie 2021).

United Nations Office on Drugs and Crime. 2020. Victims of intentional homicide, 1990-2018. https://dataunodc.un.org/content/data/homicide/homicide-rate (geraadpleeg op 25 November 2020).

Weaver, C.E., Lazaros, E.J., Zhao, J.J., Davison, C.B., Truell, A.D. 2020. The Internet of Things: An overview of selected smart home technology. Issues in Information Systems, 21(2), 43-48.

World Bank. 2020. South Africa. https://data.worldbank.org/country/ZA (geraadpleeg op 24 November 2020).

Yassein, M.B., Mardini, W., Almasri, T. 2018. Evaluation of security regarding Z-Wave wireless protocol. In: Proceedings of the Fourth International Conference on Engineering & MIS 2018 - ICEMIS ‹18. The Fourth International Conference, New York, New York, USA: ACM Press, 1-8. https://doi.org/10.1145/3234698.3234730.

Yoffie, D.B., Wu, L., Sweitzer, J., Eden, D., Ahuja, K. 2018. Voice War: Hey Google vs. Alexa vs. Siri. Harvard Business School Case 718-519, 1-25.

Zinn, R. 2008. The modus operandi of house robbers in the Gauteng Province. Acta Criminologica: African Journal of Criminology & Victimology, 21(2), 56-69.