IoT AND PRIVACY BY DESIGN IN THE SMART HOME

Author:
Tony Anscombe

Researchers:
Juraj Bartko, Ivan Bešina, **Miloš Čermák,**
Milan Fránik, Štefan Svorenčík, **Kacper Szurek**

ENJOY SAFER TECHNOLOGY™

CONTENTS

1. ABOUT THE INTERNET OF THINGS

The Internet of Things (IoT) has become a globally recognized term in workplaces and homes, and in a literal sense could be used to describe anything that is connected to the internet. However, if you ask what sort of devices are included in the IoT, then you are likely to get differing answers with respondents describing the devices they have come into contact with, or know about. This can include everything from cell phones, smart bulbs, fitness trackers, smart speakers and dishwashers, all the way to water quality sensors in pumping stations.

When predictions on the proliferation of IoT devices started to emerge, we heard huge numbers from analysts. 50 billion by 2020 was the number quoted in a presentation by Ericsson's former ***CEO Hans Vestberg*** in 2010. Eight years later the initial hype around the industry sector has subsided and the numbers cited are more conservative. Today, Ericsson offers a more nuanced view, ***estimating that around 29 billion connected devices are forecast by 2022, of which around 18 billion will be related to IoT***.

While the numbers game will remain ongoing, what is certain is that many of these devices will be consumer gadgets which may bring numerous benefits to households, but may also threaten consumers' privacy and security. The sensors packed into Smart Home products – with their microphones, cameras, interface with GPS, not to mention interoperability – are juicy targets for malware attacks. By gaining control over these devices, cybercriminals can not only attack other devices on a user's network but also spy and gather sensitive and personal data.

A team of enthusiastic researchers at ESET has investigated some these popular IoT devices such as cameras, scales, sensors and home management systems. This white paper details the research they carried out and looks specifically at privacy concerns relating to the creation of a

basic smart home. Where obvious issues relating to a specific device have been found we do, of course, mention them.

As there is no widely agreed definition of what constitutes a 'smart home', we decided to focus our attention, for this white paper, only on IoT devices apparently aimed primarily at the consumer market.

Arguably, a truly smart home would require a major remodel and significant initial financial commitment to create an intuitive and automatic environment that anticipates and adapts to the changing lifestyle of the occupants in real time. The attraction for consumers is to save energy and long-term expenditure while increasing comfort and convenience.

Alas, this is probably a commitment out of reach for many, or at least for today. The smart home for most of us will be a small foray into the world of IoT, with a limited number of well-placed devices that add convenience, comfort or novelty. One of the challenges facing even the most basic implementation of a smart home is interoperability between devices from different manufacturers to provide a harmonious, unified experience.

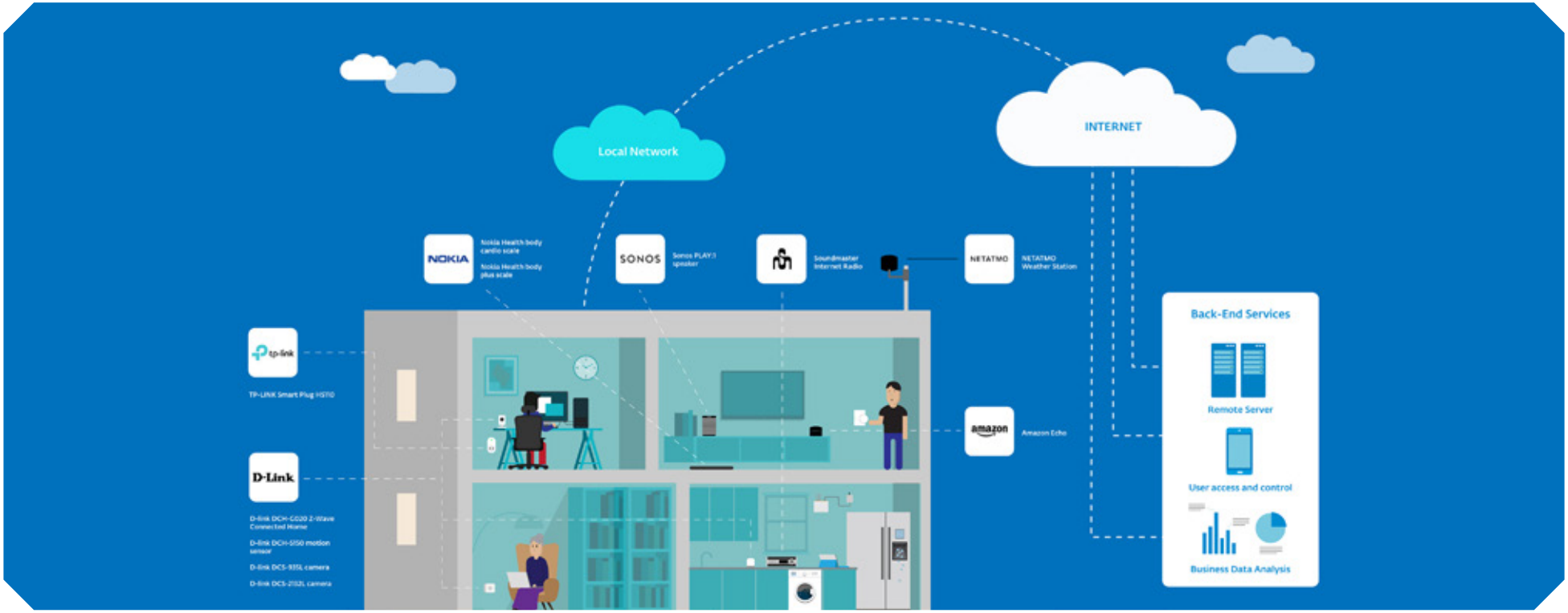
Each device provides a feature set designed to inform us about our activities or enables us to perform an activity. There are, or should be, concerns about the risks to individuals that arise from possibly inadvertently or inappropriately sharing data about personal movement or lifestyle. The sheer volume of such data shared nowadays fully justifies these concerns.

A single device risk was highlighted recently by Nathan Ruser, a 20 year old Australian university student who is studying international security at the ***Australian National University***. In a tweet on January 27, 2018, ***Ruser highlighted*** an operational security issue for military personnel using a fitness app from ***Strava***. The app uses GPS location in cell phones to track routes for jogging, cycling or other fitness activities. By default, users allow anonymized sharing of their data so that Strava can produce a heatmap showing popular routes. The example highlighted by Ruser was the Bagram Air Base in Afghanistan, showing the regular jogging routes used by US military personnel stationed there. This is a good example of a popular app collecting data and aggregating it to produce some useful and very cool output, but in this case raising obvious security issues. Attempting to find a route to jog when away from home is now simple, but the consequences to security and privacy are not immediately apparent.

2. THE SMART HOME

Each 'thing' in the term 'Internet of Things' refers to a device, and there are many types of connectable device, from cameras, scales, sensors, and home management systems, all the way to heart monitoring implants to cars or sensors monitoring livestock. The opportunities for interconnection are endless. For example, San Jose, California, has committed to ***creating a smart city*** that they claim will deliver the safest and most inclusive, user-friendly environment for its residents. The project promises to use an IoT platform employing transit vehicles and an infrastructure of smart sensor technologies to improve safety, mobility and optimization of the transit system.

Science fiction writers once envisioned a world regulated via the interconnected devices used in everyday life. Today such a world is fast becoming reality. Take, for example, a security camera that starts recording when a motion sensor is activated and alerts your phone. Already we have a number of devices involved in maintaining a cloud-based service. In simple terms there is the device, the network to which it is connected, the device that controls or interacts with it – most probably a smartphone – and then there is the cloud service that either stores the data from it or is acting as a conduit to deliver the data to the phone. Potentially, one more



component, a home management system comprising a master device or hub might be deployed, providing a single interface to manage connected devices that provide services around the home.

There are several main scenarios for controlling and communicating with devices. As consumers, we are familiar with at least two of them: Bluetooth and Wi-Fi. If for example there is a device that only needs to be controlled locally by a smartphone, then a short-range wireless technology such as Bluetooth or Wi-Fi could be used. In home automation systems where a hub is used, it is common to find one or more of the Z-Wave, BidCoS and ZigBee, communication protocols that provides low-latency data transfer and power consumption lower than Wi-Fi. The hub is then connected through Wi-Fi or wired Ethernet, allowing connection from remote devices or cloud services.

3. THE PRIVACY POLICY AND DATA CAPTURE

Each manufacturer should have a privacy policy or similar document explaining how the data captured by a device, or through its associated services, that you use is collected and used. Some of the policies are vague and hard to read and in some cases difficult to locate, while others demonstrate exceptional efforts by companies to make them readable and understandable.

Companies also have a tendency to make privacy policies cover a wider range of eventualities than may arise in reality, so they may not be collecting all the things stated in the policy. The policies are complex documents that require considerable legal resources to write, modify and maintain, so listing everything you might collect is seen as a method of future-proofing the policy. It does, of course, mean that if you accepted the policy today, then the company could be collecting the listed data tomorrow.

We are not questioning the reasons for, or other aspects of, data collection for this paper; we're taking a holistic view of the data being collected overall in order to provide services in a basic smart home. Looking at the quantity and depth of data collected raises concerns that an individual is oversharing unwittingly.

It is understood that most devices and services will collect basic personal details that may include given name, address, date of birth, email and phone number. The data included for each device are taken from the applicable privacy policy published by the company concerned. Often companies use the term 'but not limited to', meaning that if they want, they can collect more than what is described on the list.

When devices are controlled by a service other than the one offered by the vendors that created the devices, then data could be collected by the third party service provider as well. For example, the D Link products that use the cloud service can also be controlled by Amazon's Alexa. A simple command such as 'Alexa, tell mydlink to switch on the garage camera' may mean that both mydlink and Amazon are aware not only of the instruction, but of what device it operates and how it is used. The consequences of all commands sent to various devices from different vendors flowing through a single party could add up to greater convenience for the end user, but some may see this as one entity able to build up a full lifestyle profile on the household and its occupants.

4. VULNERABLE DEVICES

Did we find vulnerabilities? Yes.

We initially chose and tested twelve products from eight vendors: the details of eleven products from seven vendors are included later in this white paper. The product that is missing from this paper had significant vulnerabilities. As a security company we value the commitment to responsible disclosure and the collaborative nature of the IT security industry — therefore, we notified the company in question with specific details of this device's vulnerabilities. That device is a home automation control panel that can manage motion sensors, heating controls, shutter motors, environment sensors and smart plugs. The device has a number of vulnerabilities, including:

- *The login process from the local network is not fully authenticated. The default option is to allow auto-login, which bypasses the need for standard credentials such as userID and Password. The manufacturer does mention this issue in a security alert, and recommends disabling this default option.*

- *As with nearly all smart home systems, a cloud service provides the functionality to manage the connected devices from one place. The communications to the cloud service are not encrypted.*
- *The vendor's cloud service has the ability to establish a virtual private network (VPN) connection to the remote devices. Once this tunnel is established, it could be possible for the remote network configuration to be changed. This could result in the users' local network being accessed without consent.*
- *Accessing the cloud service requires registration, but if the user details become compromised the VPN access to the remote network could present a considerable risk.*

The remaining devices that we tested and detail in this paper demonstrate the need for research and investigation before making a decision to purchase. For example, the ***D-Link cameras*** and the ***TP-link Smart Plug*** have well documented security issues. The main concern with cameras is the lack of encryption of the video stream coupled, in this case, with weak authentication.

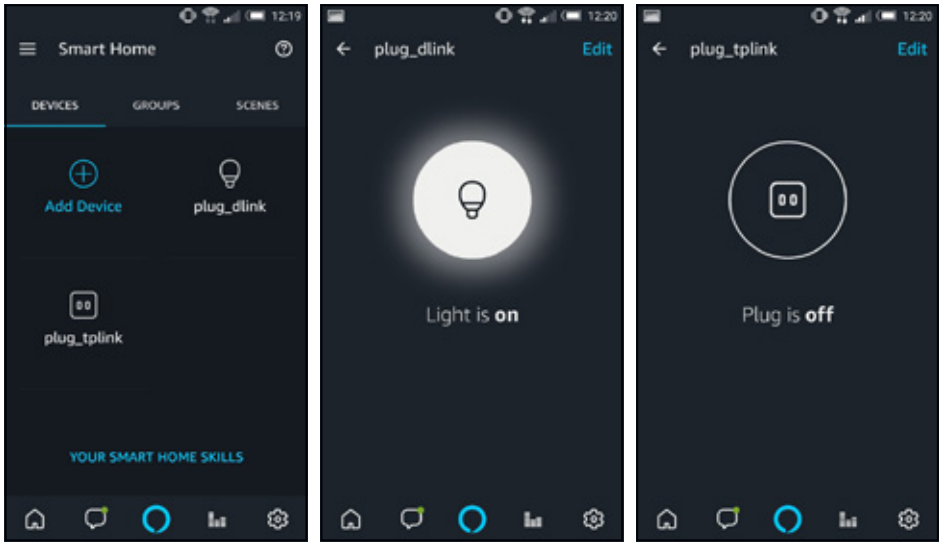
There are cameras available that are secure and encrypt the video stream, both in real-time and when stored. The devices we tested were from a recognized brand, which suggests that 'name brand' does not necessarily mean secure, at least where cameras are involved.

5. PRIVACY, THE BIG CONCERN

Are there privacy concerns? Yes.

Each device in the test collected different data to facilitate its functionality and in most cases the data collected seemed in context with the service being provided. The Soundmaster Internet Radio, without an obvious privacy policy and with a lack of any meaningful terms, raised a red flag for our researchers. If there is no stated policy, then no informed decision can be made.

The most significant concerns are raised by voice-activated intelligent assistants — in this instance Alexa. A service that acts as a conduit to all other devices and then stores the interactions with them, potentially creates a single treasure chest for a cybercriminal. Neither the reputation of the device nor Amazon's services are in question, but a smart hacker trying to harvest personal data for identity theft could create a spear-phishing attack on individuals to gain access to their Amazon accounts.



he screen images above are examples of the Alexa app's Smart Home functionality.

Alexa – can you be secured? Possibly.

If you decide to utilize this polite and obedient intelligent assistant, then configure it ***with some parameters***.

- *Require a PIN when purchasing through voice, or better yet don't purchase through voice.*
- *Train Alexa to know your voice and then limit functionality to only your recognized instructions.*
- *When you don't need an assistant, switch it off, or at least mute the mic.*

6. ESET TEST: THE IOT DEVICES IN OUR 'BASIC' SMART HOME

a. Amazon

Amazon Echo (2nd Generation)

The Amazon Echo is a hands-free, voice-activated, virtual assistant that uses the Amazon Alexa service to answer questions or to allow you to give commands such as to play music, set alarms or to control smart home devices that are Alexa-compatible.

Seven microphones and noise cancellation ensure that Alexa can hear your commands from across a room even when music is playing.

With 360 degree omnidirectional audio it can fill the room with music that benefits from Dolby processing and dynamic base response.

A growing number of vendors are adding support for Alexa through 'skills' which gives the device control of other devices and services to bring together the smart home into one verbally controlled device.

Alexa Terms of Use

https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740

Alexa enabled products collect and send to Amazon:

Your Alexa interactions
Voice inputs
Music playlists
Your Alexa to-do and shopping lists.
Device type
Name
Features
Status
Network connectivity
Location

Amazon may automatically update the firmware for certain auxiliary products on behalf of the applicable manufacturer.

Note: This does not included details of Amazon's general privacy policy, only the details of the Alexa service.

Security & Privacy

If you own an Amazon Echo then your best friend may well be Alexa, a device to which you can pose an unlimited number of questions, as well as give it instructions and receive polite and prompt responses. When setting up a smart home, it is probably a must-have device. The device can perform a wide range of services both directly or through connections you approve to third parties, including playing music, reading the news, checking your calendar and putting together your to-do list, and of course purchasing things through your Amazon account.

The Echo is constantly listening for your commands and is voice-controlled, sitting dormant until it recognizes the 'wake word'. This word brings Alexa to life and allows you to give a direct command or a command tied to a skill (see next paragraph). The instruction is transmitted to Amazon for analysis and a response is generated. These interactions are associated with your Amazon account and can be reviewed.

If the interaction is related to a third party – for instance, you are asking Nokia's Health Mate app how much you weigh – then Nokia does not get the audio request, just the request for your weight. To make this interaction possible, there is a requirement to connect the third-party account to Alexa in order to make the information available. This is referred to as an 'Alexa skill'.

The audio interactions are stored in, and associated with, your Amazon account. You can delete them either one at a time in the Alexa app, or in blocks through Amazon's website. Are users engaged enough to review what is being stored and to delete anything that may be deemed personal? Probably not.

The data could be enlightening to a marketer. Your interactions will have informed Amazon what products you like to purchase and from whom, what you listen to, what other connected products you have, and so on. This collection of data enables a profile to be built that potentially contains very specific details about your lifestyle – a marketer's dream, and potentially a cybercriminal's too. It is important once again to emphasize that you are in control and there is nothing hidden here since you can see the interactions and delete them. Also, if you become too concerned then you can always switch Alexa off, either fully or by just muting the microphone.

With data breaches frequently in the news, any voice-activated digital assistant could be a reason for concern. If, for example, someone gains access to your Amazon account name and password, they have the ability to listen to your interactions with Alexa. The depth of information stored in the interactions could cause embarrassment as well as be a privacy issue.

There are precautions you can take:

> - *Set up voice recognition so only you can use Alexa, which will stop visitors to your house having fun with it*
> - *Delete the recordings of past interactions*
> - *Consider not connecting other devices when the data is deemed to be too personal*
> - *Switch off Alexa when you don't need it*
> - *Protect your Amazon account with two-factor-authentication. This prevents access should your login details inadvertently fall into the wrong hands*

b. D-Link

D-Link DCH-G020 Connected Home

The DCH-G020 is a Connected Home Hub that is a central conduit to link all of your existing mydlink Wi Fi and Z Wave devices. When used in combination with home sensors it can alert you when doors or windows are opened or when motion is detected. With the cloud service mydlink Home it can simplify setting up a smart home without the need for additional subscriptions or charges.

D-Link DCH-S150 Motion Sensor

The DCH-S150 Motion Sensor detects motion and can be paired with other devices to take predefined actions, for example, when paired with a camera, video can be captured, or paired with a Smart Plug it could switch on lighting. Notifications and alerts can be sent to mobile devices or through email.

D-Link DCS-935L Camera

The DCS-935L Camera is a connected camera that can capture clear crisp images. It boasts 720p HD video quality, night vision up to 16 feet and has both sound and motion sensing technology. Notifications and alerts can be sent to mobile devices or through email. Remote viewing is free through web browsers and mobile devices when viewed through D Link's cloud service mydlink.

D-Link DCS-2132L Camera

The DCS-2132L provides the ability to directly transmit high quality video images for security and surveillance or other purposes. It hosts its own web server and has a built in CPU which means it can be accessed from any web browser over the internet. The integrated device has infrared for night video, motion detection, a microphone and a speaker.

'mydlink' is a cloud service providing configuration, control and monitoring of all of your compatible D Link devices. Accessed through mobile device apps or a web browser, it provides a single, central location to view cameras or to see the status of the smart home network.

Privacy Policy

https://www.mydlink.com/privacyPolicy

Each mydlink product will collect some or all of the following:

- Voice
- Sound
- Face
- Temperature
- Ambient Light
- Humidity
- CO2 Levels
- Precipitation
- Moisture
- Noise decibels
- Motion from sensors
- Utilities usage data
- App Settings
- Scheduling
- Alerts
- Notifications
- Product location in premises
- SSID (Wi-Fi Name)
- Wi-Fi password
- Audio and Video signals

Amazon Echo Enabled

Yes

Security & Privacy

Communication from a mobile device to the mydlink cloud service is encrypted and the connection between the device and the D Link servers is also encrypted.

However, firmware updates are delivered by http rather than by https, which means an attacker could inject malware into the update since the data stream is not encrypted. Our attempt to take control or change the operation of the device by creating a modified update resulted in its failing to be installed. This is evidence that checks on the update package are taking place despite the fact that the data delivered is not encrypted. Interestingly, changing just a few unimportant bytes did not stop the update from taking place.

The cameras included in the ESET smart home test do have weaknesses, some of which have been documented in other tests. For example, AV

Test in Germany tested the D Link DCS-2132L and awarded it only one star out of five, noting a number of significant security issues. One year later there are still issues, such as basic http authentication and video stream encryption remains insufficient and reversible, as well as accessible over a public IP address. However, the camera is controlled from the mydlink app, which is encrypted. But if the video stream itself is poorly protected, then the security and privacy concerns centre on the content being captured. If a camera is used to monitor surfing activity at a beach then it could be argued that reversing the encryption to see how big the wave is would be a waste of time and effort. However, a camera placed in the home would have very different security and privacy implications.

It is disappointing that after a thorough examination by AV Test in January 2017, the issues remain largely the same 12 months later.

c. NETAMTO

NETAMTO Weather Station

The NETAMTO Weather Station has two modules: an outdoor module provides real time access to weather conditions while an indoor module monitors conditions indoors such as air quality. Knowing the exact conditions before heading off to the cabin for the weekend could prove very useful. Through a crowd sourced network of NETAMTO devices, you can see local condition variances and conditions in other locations.

Privacy Policy

https://www.netatmo.com/en-US/site/terms

The NETAMTO privacy policy is not as detailed as some of the others. The wording is generalized and is about categories of data rather than specific examples of what actual data is collected. This means users may be unaware of the reality of what is being collected, stored or shared.

However, when purchasing a NETAMTO Weather Station, one of the key buying propositions is the Weathermap (see the link and description below).

When you use the services, there is automated collection of:

> Personal data and measurement
> Usage
> Your activity with services
> IP address

NETAMTO share aggregated anonymized personal data with third parties

Amazon Echo Enabled

Yes

Security & Privacy

NETAMTO provide a Weathermap so you can see the weather in any location where a device is installed and shares its findings. If you choose to contribute to the Weathermap then the data from the external sensor will be shared. Your internal data remains private. If you choose not to share then only you will see your device on the map.

If you do decide to share the data from your device, then the location is specific. Take a look using the Weathermap link above and select one of the devices. The street address is shown in the details on the right. The only thing missing is the house number. Opening a Google map in another browser window and comparing could potentially enable you to ascertain the actual address.

Is sharing the address a cause for concern? Yes. Ever received a call saying that an issue has been identified with your laptop or Windows? If you have, then it came from one of the many tech support scams designed to charge

you for a service that you did not need. Imagine the call being a little more specific and no longer guessing whether you have a laptop running windows and instead the caller asking specific questions about your weather station. This validated knowledge about what devices are installed at your location may make it significantly harder to detect a fraudulent call.

NETAMTO did have issues with plaintext Wi-Fi credentials being communicated, back in 2015. They resolved these issues with a firmware update. Once connected, the device automatically downloads the latest firmware version from the cloud. While not delivered over SSL, it is encoded using a proprietary method.

d. Nokia Health

Devices

Nokia Health Body+ Scale

The Nokia Health Body+ Scale is far more than a bathroom scale. It can accurately provide additional information such as body mass index, body fat, water percentage, muscle and bone mass. With the Health Mate app you can track progress and get coaching advice to help reach your objectives.

Nokia Health Body Cardio Scale

The Nokia Health Body Cardio Scale adds additional functionality over the Nokia Health Body+ Scale and can track your cardiovascular health via a heart rate monitor.

Privacy Policy

https://health.nokia.com/us/en/legal/privacy-policy

When you are using Nokia digital health Products and Services, the privacy policy states that Nokia may need to collect:

Identity Data

> IP address
> Videos and pictures of you

Activity Data

> Your number of steps
> Distance travelled
> Number of swimming strokes
> Number of calories burned
> Type of activity
> Level of activity
> Sport session time

Body Metrics Data

> Your weight
> Muscle
> Fat
> Health rate
> Breathing rate
> Blood pressure

Environmental Data

> Noise level
> Light level
> Temperature level
> CO2 concentration

Positioning and location Data

Amazon Echo Enabled

Yes

Security & Privacy

Privacy with health-related data should be paramount. Nokia's privacy policy states:

Some services may allow you to share your personal data with other users of the service or with other services and their users. Please consider carefully before disclosing any personal data or other information that might be accessible to other users.

When you look at the personal nature of the data collected, then sharing may seem inappropriate: however, someone on a drive to lose weight may, of course, be motivated by sharing information on steps walked or weight lost. In general, once data is shared, even with other family members or friends, it should be considered to be public, as you have passed control to someone else.

The ESET research team took a deeper look at the device because of the type of data collected, and the team's actual comment was "the security of this device was relatively good". We set out to attempt to access the data flowing between either the scale or the Health Mate app and the cloud service they communicate with and the affiliated cloud service.

It was possible to launch a man-in-the-middle (MitM) attack between the Android app and the cloud, but to achieve this the Android device needed to be rooted and a MitM root certificate needed to be installed. As the scale communicates with the Android device and firmware updates are delivered through the app, the MitM attack allowed us to intercept the firmware updates. The download is encrypted using SSL, then ultimately flowing through the Android device to the scales. Modifications to the firmware could be made and then written to the scales over the Bluetooth connection, but to do this a setup mode button needed to be pressed on the scales, meaning you needed to be physically next to them so a remote attack was not a factor.

Modifying the firmware to downgrade the communications with the scale from https to http was successful. The data being transmitted was then readable. Even then, though, the data and parameters being transmitted are not easily ascertained.

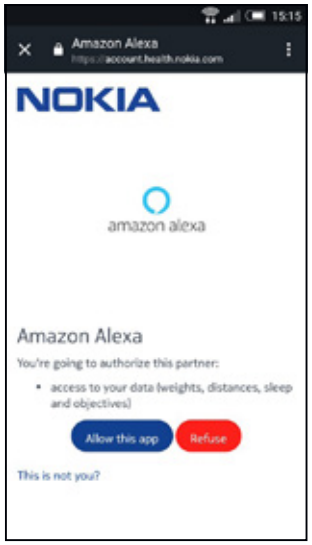
In summary, it is highly unlikely to find a scenario where a hacker can access the phone, root the device, intercept the firmware download, rewrite it, then press a magic setup button on the actual weighing scale and install the new firmware. And if they did, the data they could see is meaningless without extensive further reverse engineering.

One other curious feature of the scale is a weather forecast. Yes, you are reading this correctly. If the scale knows your location, which is established from your phone, then a local forecast is available on the scales display while you weigh yourself. Whether this is a security or privacy risk remains to be seen, but sharing your location with your scale's seems out of context.

The biggest risk with the scales is that users might overshare their own data through social media networks, or that a third party might get access to sensitive personal information. The third party focused on in this paper is the Amazon Echo. When linking the Nokia Scale to the Amazon Echo you can ask Alexa questions about the data stored in your Health Mate account. On the Amazon web page that details the Nokia skill and offers enablement, there is the following statement:

https://www.amazon.com/Nokia-Apps-Distribution-LLC-Health/dp/B0786NLDBF

Note: Alexa and Amazon, Inc. do not store or retain your Nokia Health data, but voice interactions associated with your Amazon account may contain your Nokia Health Mate data.



When you link Alexa and grant Amazon permission to access your Nokia Health Mate account, the screen above is displayed. Note that it is specifically mentioned that you are granting Amazon Alexa access to personal data including weight, distance, sleep and objectives.

When asking Alexa your weight, the privacy policy statement should give you confidence that Amazon is not storing the data from your Nokia Health Mate account. However, they are storing it in the form of voice interactions associated with your Amazon account. Remember, if you access your voice interactions in the Alexa app then you can see all the interactions in written form, and you can play the original audio back. You do have control and can delete these interactions and can optionally review the accuracy of the Alexa interaction.

The issue with placing control back in the hands of the user to delete these interactions is that many will not know they are stored and even if they do, then deleting them is a task likely to be both arduous and infrequent.

e. Sonos

Sonos PLAY:1 Speaker

The Sonos PLAY:1 is a Wi-Fi-connected speaker that can stream music regardless of the status of your mobile device. No more interruptions due to an interruption in Bluetooth connectivity. Combined with an Amazon Echo or Dot you can verbally control the tune, playlist or radio station that is playing. Multiple speakers in different rooms can be synchronized to play the same song or everyone can be enjoying a different tune at the same time.

Privacy Policy

https://www.sonos.com/en-us/legal/privacy

The policy states that Sonos may collect:

Product type
Controller device type
Operating system of controller
Software version information
Content source (audio line in)
Signal input (example – Dolby)
Information about Wi-Fi antennas
Audio settings
Product orientation
Room names you assign
Tuned using Sonos Trueplay
Temperature of your product
Wi-Fi information (signal strength)
Music services you connect to (for some services login username – but not password)
How often you use the Sonos app vs another control mechanism
Flow of interactions within Sonos app
How often you use physical controls on the unit
Location data when app is in use
Duration of use
Duration of music service use
Product and room grouping information
Command information, play, pause, change volume, skip tracks, information about tracks, playlist, station container, Sonos playlist, Sonos favorites

Amazon Echo Enabled

Yes

Security & Privacy

It is important to note that this device is a Wi-Fi-enabled speaker as opposed to Bluetooth-enabled. This removes the necessity for a paired device, for example a cell phone, to be in a certain proximity and allows the phone's audio functions to work independently.

The Sonos or other app that is aware of the device's existence, broadcasts a network wide desire to play audio. As the speaker is in permanent listening mode, it will see this request being broadcast and play the requested audio.

A Sonos account is required to work with the app. The speaker frequently connects to Sonos servers. There are two connections: one is a permanent connection while the other is an hourly connection. Both are protected with encryption. The permanent connection is not surprising as the speaker works with Amazon's Alexa. Asking Alexa to play a track on your Sonos speaker would require a connection between Sono's servers and the speaker so the track can be streamed.

Sonos's privacy policy states that interactions with the app and music services to which you connect are captured. This is to be expected, as nearly all music services offer recommendations on music you may like.

The policy also states that room names you assign to the device are stored. This is understandable as you need to be able to specify what device you want to play a track on, "Alexa please play 'Beautiful' by James Blunt on the kitchen speaker". If someone gained access to this data, that could possibly be an overshare, depending on what you have called the rooms. If for example you have speakers in your children's bedrooms, then naming the speakers using your children's names may be inadvertently sharing data with Sonos about the people in your family.

There is a new version of the speaker available, the Sonos One. This combines the functionality of the speaker and the Amazon Echo. The Sonos speaker in effect takes the role of being an Amazon Echo. In this scenario, Sonos's privacy policy is clear that interactions with Alexa are not retained by Sonos.

f. Wörlein

Soundmaster Internet Radio IR4000SW

This modern designed internet radio in appealing black lacquer look with practical carrying handle is the perfect companion for those who are looking for a radio that leaves nothing to be desired. The internet radio IR4000SW in white also supports the reception of DAB + and FM PLL radio, whereby your favorite stations can be stored by preset memory and are thus easily accessible. The device is connected via Wi-Fi to the internet. In addition, a USB port is add this available. [Description translated from amazon.de.]

Privacy Policy

We could not find a privacy policy related to the products of the company. There is a German language privacy policy for visitors to the company website, here. However, for an English- speaking visitor to the website, the policy is still displayed in German. You can buy products in English but not read the policy. There is, of course, Google Translate, but nuances may be lost in translation – particularly important for legal documents.

Amazon Echo Enabled

No

Security & Privacy

With no privacy policy, we need to rely on our investigation to understand what communication is happening between the device and the internet. Firstly, when configuring the device to connect to the Wi-Fi network the password is not obscured once typed so anyone who can visually observe it being configured, can see the password in clear text. If the

device is accessible, for example in a public place such as an office or retail establishment then the Wi-Fi credentials would be accessible by clicking through the settings. If a company creates products with security by design as a prerequisite, then a password being displayed in clear text or accessible without authentication is unlikely to occur.

When selecting a radio station, an instruction is sent in clear text to mediayou.net, which appears to be a portal for accessing online radio content. mediayou.net will know the IP address of the radio connecting to it, the requested radio station, and the time and duration of listening.

There is no privacy policy listed on the mediayou.net website. Even when creating an account on the site there was no offer of any privacy policy or terms of use. Researching the mediayou.net domain to establish who owns it is futile, as the domain details are hidden behind a privacy shield, which is a little ironic.

Without any understanding of what, if any, data may be collected and retained, then you have to assume the worst case: that is, that a company will collect everything they can and sell it to whomever and however they choose. At a time when personal data has value and identity theft is a growing issue, this is an unacceptable situation.

g. TP-Link

TP Link Smart Plug HS110

The TP Link Smart Plug allows you to connect a standard non-smart device and control the power to it directly from your smartphone. Remotely switching on a fan, the lights or boiling a kettle without having to replace the devices with new, smart, connected devices is a cost-effective way to start a smart home.

Privacy Policy

http://www.tp-link.com/us/privacy

The policy states that TP-Link may collect:

Firmware version
IP address
MAC address
Other identifying information, such as names and images that associate you with account users
Your location
Devices
Scenes
Device configuration details
Demographic information
Third party account details
Schedules
Audio/Video recordings
Third party device usage, such as when a motion sensor senses motion
Type of device or service information is received from
User configurable device name, group name, location name
IP Address
Location

Mobile device information

Amazon Echo Enabled

Yes

Security & Privacy

When we set out to create our basic smart home, we selected devices by price, availability and a perception of popularity. Taking a device that may not itself be connected or 'smart' and controlling it through its power source is both cost effective and convenient. For example, you may want to boil a kettle of water without the need to actually visit the kettle. Imagine that before heading to bed you flip the switch on the kettle to 'on' and when you wake up you switch on the power to the socket remotely or through a voice activation service such as Amazon Alexa.

This device has well-documented vulnerabilities that include easily-reversible encryption between the device and the TP Link Kasa app used to control it, certificate validation issues and potential man-in-the-middle attacks.

On January 5, 2018, TP Link published a vulnerability statement detailing issues with WPA2 Security due to KRACK. However, KRACK is an industry-wide issue and the details were widely disclosed in October 2017 by the two researchers who found the flaw. The HS110 is shown in the TP Link statement as having been fixed if you are running the correct firmware, which is delivered through the Kasa app.

Searching online for 'tp link hs110 vulnerabilities' over 2600 results. The content of the results page should raise a red flag to a potential purchaser. In the first few results, ignoring the KRACK items mentioned above, you see terms such as 'Reverse Engineering the TP Link HS110…', 'TP LINK HS110 weak authentication…' and 'Hacking TP Link devices…'.

Purchasing an inexpensive device in an attempt to use an otherwise non-connectable device as part of a smart home may seem like a cost-effective solution but, as you can see in this case, it is not always without issues.

7. CONCLUSION – IS IT SAFE?

Is it safe to create a smart home? Possibly.

At its inception, the goal of this project was to create a basic smart home that mimics something that could end up in typical household. The concern from our research team was "what if we don't find any issues?" What a great leap forward it would be for IoT if we actually had found no concerns, and our recommendation to all who feel the need to start building that smart home was to 'go right ahead!'. Alas, this is not the case, and in fact the conclusion that I am writing now is different from what I had envisioned at the start.

No device or software is guaranteed secure or without potential vulnerabilities. However, companies can be judged based on how they react to disclosure of vulnerabilities in their products. Some of the devices tested had vulnerabilities that have been dealt with quickly with new software and firmware. Unless such disclosures are promptly acknowledged and the vulnerabilities fixed, choosing an alternate device would be an appropriate response. By using sound judgement and caution it is possible to start building a basic smart home. Below are the main considerations we would suggest that you follow before purchasing components or starting out on this journey.

- *Researching potential vulnerabilities before purchasing should be a mandatory requirement before making a decision. A simple search as per the examples below will give you an indication if there are known issues.*

Device name security vulnerability
Device brand name security vulnerability
Device brand name privacy breach
Device brand name data leak

- *Does the manufacturer update the firmware and can it be auto-updated, or at a minimum, notify you through an app or email? Check the vendor website or perhaps search online to find the information.*
- *Read the privacy policy. Understanding what data is collected, stored or shared will help you make the decision on whether the device should be part of the overall network or kept isolated. And if neither of these is deemed secure, then of course don't purchase.*
- *Use caution when sharing data on social networks or with a vendor's own systems. Sharing your location, device and pattern of usage may give cybercriminals enough data to scam you or start a targeted attack.*
- *Voice-controlled intelligent personal assistants are convenient. They are also all-knowing. Think carefully how much you tell your assistant, or how much you ask it to gather on your behalf.*

Each person reading this paper will have a differing view on what personal information they are willing to disclose, either to a single vendor or to a company that has an aggregated view. The potential for home, lifestyle, health and even browsing data collected by internet service providers to be available to a single entity should only be permitted after due consideration for the consequences. As companies discover new ways to monetize data collected by IoT devices, then either the industry needs to self-regulate, or governments will need to strengthen privacy legislation in a similar way to that in which the EU has implemented GDPR.

February 2018

ESET, spol. s r.o.
Aupark Tower, 16th Floor
Einsteinova 24, 851 01 Bratislava
Slovak Republic