Surviving in an IoT-enabled world

How to Use Smart Devices and Stay Safe from Hackers

By Victor Alyushin, Vladimir Krylov on November 5, 2015. 10:59 am

Scare stories around the Internet of Things (IoT) conjure up images of bad guys in hoodies, who live for hacking and to make the lives of other people harder, inventing millions of ways to infiltrate your life through your gadgets. But is this perception a good enough reason to stop using smart devices? We don't think so; we believe that customers should be aware of the potential risks and know how to mitigate them before embracing the IoT-enabled world.

More than a year ago, our colleague from the Global Research and Analysis Team, David Jacoby looked around his living-room, and decided to investigate how susceptible the devices he owned were to a cyber-attack. He discovered that almost all of them were vulnerable. So, we asked ourselves: was that a coincidence, or are the smart 'IoT' products currently on the market really that exposed? To find the answer, earlier this year we gathered up a random selection of connected home devices and took a look at how they work.

The devices we chose for our experiment were as follows:

- a USB-dongle for video streaming (Google Chromecast);
- a smartphone-controlled IP camera;
- a smartphone-controlled coffee maker; and
- a home security system, also smartphone-controlled.

The task we set ourselves was simple: to find out whether any of those products posed a security threat to their owner. The results of our investigation provide much food for thought.

Google Chromecast. IoT hacking for beginners

Risk: the content on the victim's screen is streamed from a source owned by an attacker

Chromecast, which has been recently updated with a more advanced version, is an interesting device. It's an inexpensive USB-dongle that allows you to stream media from your smartphone or tablet to a TV- or other display-screen. It works like this: the user connects it to a television's HDMI in order to switch it on. After that the Chromecast launches its own Wi-Fi-network for initial setup. Once it has established a connection with a smartphone or a tablet, it switches its own Wi-Fi off and connects to the user's home Wi-Fi network. It's very convenient and user-friendly.

But this could become less convenient and decidedly unfriendly if there is a hacker nearby. The famous “rickrolling” vulnerability, discovered by security consultant, Dan Petro, proves that. It allows the content on the victim’s screen to stream from a source owned by an attacker. This is how it works: the attacker floods the device with special ‘disconnect’ requests from a rogue Raspberry Pi-based device and then, as the Chromecast turns on its own Wi-Fi module in response, Google Chromecast is reconnected to the attacker’s device making it stream the content the attacker wants.

The only way to get rid of this is to switch off the TV, take the dongle out of range of your Wi-Fi hotspot and wait until the attacker gets bored and goes away.

The only limitation to this attack is that the attacker needs to be within range of the Wi-Fi network to which the target Chromecast is connected. However, we discovered in our own experiment that this not necessarily a restriction if you have a cheap directional Wi-Fi antenna and some Kali Linux software. When we used that, we found that Chromecast can be “rickrolled” across a far greater distance than the normal signal range for domestic Wi-Fi networks. What this means is that, while in the original hack by Dan Petro, the attacker would run the risk of being spotted by an angry Chromecast owner, with a directional antenna that risk no longer exists.

We don’t regard this “finding” as a new security discovery; it simply extends a previously-known and so far unpatched security issue. It’s an exercise for beginners in IoT hacking, although it could be used in a really harmful way – but we’ll get to that later. First we’ll go through the other findings of our brief research.

Mitigation: Use in remote parts of your house as this will lower the risk of attacks with a directional antenna

Status: Not patched

IP camera

Issue one

Risk: attackers get access to the email addresses of all the camera users who have experienced technical issues

The IP camera we investigated was positioned by its vendor as a baby monitor. You put the camera in a nursery, download an app on your smartphone, connect the camera to the app and the Wi-Fi, and off you go: you can watch your child whenever you want, from anywhere you like.

Why would someone want to hack a baby monitor, you may well ask? Actually there are a number of recorded instances of baby monitor abuse dating back as early as 2013 (http://www.cbsnews.com/news/baby-monitor-hacked-spies-on-texas-child/) with a similar issue reported in 2015 (http://www.kwch.com/news/local-news/whitewater-woman-says-her-baby-monitor-was-hacked/32427912). So yes, there are people who, for some reason want to hack baby monitors.

When we investigated our camera (in the spring of 2015) there were two different apps available for customers that enabled them to communicate with the camera. Both contained security issues. We were later to learn from the vendor that one of these apps was a legacy app, however it was still being used by a number of camera owners. We discovered that this legacy app contained hardcoded credentials to a Gmail account.

```
public static final String EMAIL_FROM = “*****@gmail.com”;
    public static final String EMAIL_PASSWORD = “*******”;
    public static final String EMAIL_PORT = “465”;
    public static final String EMAIL_SMTP_HOST = “smtp.gmail.com”;
    public static final String EMAIL_TO;
    public static final String EMAIL_TO_MAXIM = “maximidc@gmail.com”;
    public static final String EMAIL_TO_PHILIPS = “*****@philips.com”;
    public static final String EMAIL_USERNAME = “*****@gmail.com”;
```

The vendor later told us that the account was used to collect reports on technical issues from the camera users.

The problem here is that reports were being sent to this pre-installed account from users' own email accounts. So an attacker would not even need to buy a camera; all they needed to do was download and reverse-engineer one of the apps to get access to the technical email account and to collect the email addresses of all the camera users who had experienced technical issues. Is it a big issue, that your email could have been exposed to a third party as a result of the exploitation of that vulnerability? It might be. However, realistically-speaking this vulnerability doesn't appear to be a tempting target for mass-harvesting personal information, mainly because of its relatively small base of victims. Technical issues are rare and the app was old and not really popular at the time of our research. Baby monitors are also a niche product so not many email addresses are stored.

On the other hand, if you are the owner of a baby monitor, you're most likely a parent and that fact makes you (and by extension your email address) a much more interesting target should an attacker plan a specific, tailored, fraud campaign.

In other words, this is not a critical security vulnerability but it could still be used by attackers. But that wasn't the only vulnerability we found while investigating the camera and the app.

Status: fixed

Issue two

Risk: full control of the camera by an attacker

After looking at the legacy app we moved on to the more recent version and immediately discovered another interesting issue.

The application communicates with the camera through a cloud service and communication between the app and the cloud service is https-encrypted. The application uses Session ID for authentication which is changed automatically each time a user initiates a new session. It might sound secure, but it is in fact possible to intercept the Session ID and to control the camera through the cloud or to retrieve the password for local access to the camera.

Before the app starts streaming data from the camera, it sends an http request to the cloud service:

type=android&id=APA91bEjfHJc7p6vw3izKmMNFYt7wJQr995171iGq2kk_rD4XaMEHhTXqTmFaAALjWD15bnaVcyMuV2a7zvEFdtV13QXildHQn0PCvQbPikag2CPJwPwOWWsXtP7B0S-Jd3W-7n0JUo-nMFg3-Kv02yb1AldWBPfE3UghvwECCMANYU3tKZCb2A&sessionId=100-U3a9cd38a-45ab-4aca-98fe-29b27b2ce280

This request contains the Session ID which could be intercepted as the request is unencrypted. The Session ID is then used to retrieve the current password. We found that it could be done by creating a special link with the Session ID in the end.

https://*****/*****/*****sessionId=100-U3a9cd38a-45ab-4aca-98fe-29b27b2ce280

In return for this link the cloud service would send the password for the session.

https:// *****/*****/*****sessionId=100-U3a9cd38a-45ab-4aca-98fe-29b27b2ce280

… “local_view”:{“password”:”N2VmYmVlOGY4NGVj”,”port”:9090} …

Using the password it is possible to get full control of the camera, including the ability to watch the streamed video, listen to audio, and play audio on the camera.

It is important to note that this is not a remote attack – the attacker must be on the same network as the app user in order to intercept the initial request, making exploitation less likely. However, app users should still proceed with caution, especially if they are using large networks that can be accessed by many people. For example, if the app user is connecting to their camera from public Wi-Fi, they could be exposing themselves to risk from an attacker on the same network. In such conditions it would not be hard to imagine a real-life app-usage scenario that involved a third-party.

Status: fixed

Issue three

Risk: god mode – an attacker can do anything with camera firmware

The third issue we discovered while investigating our smartphone-controlled camera resided not in the app but in the camera itself. And the issue is rather simple: a factory root password for SSH in the firmware. It is simple because the camera is running on Linux and the root password enables god-mode for anyone who has access to the device and knows the password. You can do anything with camera firmware: modify it, wipe it – anything. All the attacker needs to do in order to extract the password is to download and extract the firmware from the vendor’s website (although the attacker would need to be in the same network with the attacked device to get the URL from which the firmware is being downloaded), extract it and follow this path: \\ubifs\\home/.config. There it is: in plain text.

CONFIG_*******_ROOT_PASSWORD=”sVGhNBRNyE57″

CONFIG_*******_ROOT_PASSWORD=”GFg7n0MfELfL”

What’s more worrying is that, unless they are a Linux expert, there is no way for an inexperienced user to remove or change this password by themself.

Why the SSH password was there is a mystery to us, but we have some suggestions. The root access would be of use to developers and technical support specialists in a

situation where a customer encounters an unexpected technical problem that could not be fixed over the phone. In this case, a specialist could connect to the camera remotely, use the SSH password to get root access and fix an issue. Apparently this is a common practice for new models of such devices, which can contain bugs that were not discovered and fixed at the pre-release stage. We looked at the firmware of some other cameras from an alternative vendor and also discovered SSH passwords in there. So the story is: developers leave the SSH password in the firmware in order to have the ability to fix unexpected bugs there and then, and when a stable version of firmware is released they just forget to remove or encrypt the password.

Our second suggestion is that they just forgot it was there. As we discovered during our research, the part of the device where SSH passwords were found – the chipset – is usually shipped by a third-party vendor. And the third-party vendor leaves the SSH password in the camera by default for convenience, to make sure that the vendor of the end-product (the baby monitor) has the ability to tune up the chipset and to connect it with other hardware and software. So the vendor does this and then just forgets to remove the password. As simple as it sounds.

Status: fixed

Communications with the vendor

It wasn't hard to discover these vulnerabilities and we have to admit that it wasn't difficult to report them to the vendor and help them to patch them. The camera we investigated was branded by Philips, but was actually produced and maintained by Gibson Innovations. The representatives of the company were extremely quick to react to our report. As a result all the issues we reported have been patched, both in the camera and in the apps (Android and iOS).

This autumn, Rapid7 released a very interesting report about vulnerabilities in baby monitors, and a Philips product (a slightly different version of the camera we investigated) was on the list of vulnerable devices, with a number of vulnerabilities noted, some of them similar to those discovered in our research. But judging by the 'from-discovery-to-patch' timeline presented in the report, Gibson Innovations is one of only a few IoT vendors to treat security issues in their products seriously and to do so continuously. Kudos to them for such a responsible approach.

But back to our research.

One could say that the security issues we've discovered in the IP camera require access to the same network as the user of the camera or the camera itself, and they would be right. On the other hand, for an intruder that is not necessarily a major obstacle, especially if the user has another connected device in their network.

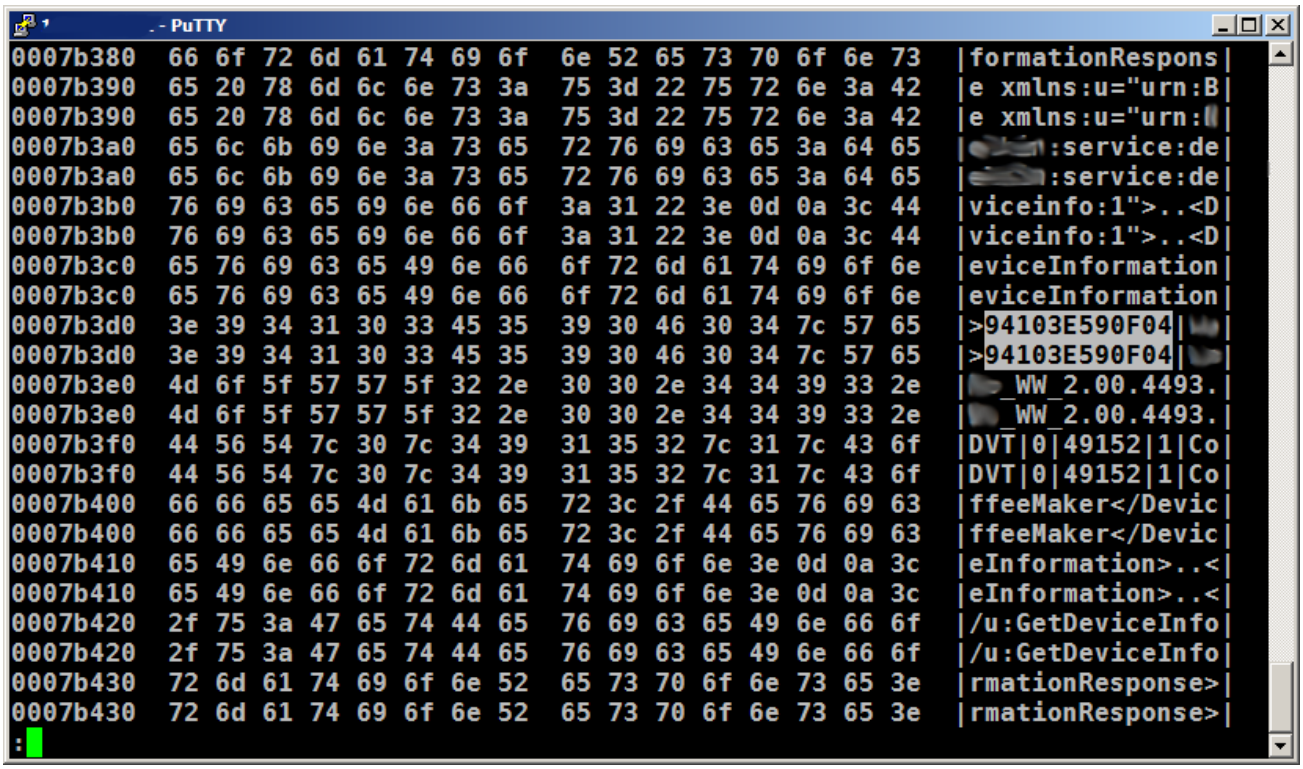
A smartphone-controlled coffee machine

What could possibly go wrong?

Risk: leakage of the password to the home wireless network

The coffee machine we've randomly chosen can remotely prepare a cup of coffee at the exact time you want. You just set the time and when the coffee is ready the app will send you a push-notification. You can also monitor the status of the machine through an app. For instance, it is possible to find out if it is brewing now or not, if it is ready for brewing or if it is time to refill the water container. In other words, a very nice device, which, unfortunately, gives an attacker a way to hijack the password of your local Wi-Fi network.

Before you use it you have to set it up. It happens like this: when the device is plugged in, it creates a non-encrypted hotspot and listens to UPNP traffic. A smartphone running the application for communicating with the coffee machine connects to this hotspot and sends a broadcast UDP request asking if there are UPNP devices in the network. As our coffee machine is such a device, it responds to this request. After that a short communication containing the SSID and the password to the home wireless network, among other things, is sent from the smartphone to the device.



This is where we detected a problem. Although the password is sent in encrypted form, the components of the encryption key are sent through an open, non-protected channel. These components are the coffee machine's Ethernet address and some other unique credentials. Using these components, the encryption key is generated in the smartphone. The password to the home network is encrypted with this key using 128-bit AES, and sent in base64 form to the coffee machine. In the coffee machine, the key is also generated using these components, and the password can be decrypted. Then, the coffee machine connects to the home wireless network and ceases to be a hotspot until it is reset. From this moment on, the coffee machine is only accessible via the home wireless network. But it doesn't matter, as by then the password is already compromised.

Status: the vulnerability is still in place

Communications with vendor

We've reported our findings to the vendor of the coffee machine, and the vendor has acknowledged the issue and provided us with the following statement:

"Both user experience and security are extremely important to us and we continually strive to strike the right balance between the two. The actual risks associated with the vulnerabilities you mentioned during set-up are extremely low. In order to gain access, a hacker would have to be physically within the radius of the home network at the exact time of set-up, which is a window of only a few minutes. In other words, a hacker would have to specifically target a smart coffee maker user and be around at the exact point of set-up, which is extremely unlikely. Because of this, we do not believe the potential vulnerabilities justify the significant negative impacts it will have on user experience if we make the suggested changes. Though no definite plans to

change our set-up procedure are in the works, we are constantly reevaluating and wouldn't hesitate to make changes if risks become more significant. Should something change in the near future we will let you know."

We don't entirely disagree with this statement and have to admit that the attack window is extremely short. The vulnerability could be patched in several ways, but based on the conclusions of our own analysis, almost all of these ways would involve either hardware changes (the Ethernet port on the coffee machine or a keyboard for the password would solve the problem) or the provision of a unique pin code for each coffee machine including those that have already been sold, which is not easy from a logistical point of view. Such changes would considerably impact the user experience and the set up process would become less straightforward.

The only software fix we can propose is to implement asymmetric encryption. In this case the coffee maker would have to send out the public encryption key to the user's smartphone and only after that the sensitive data exchange would start. This, however, would still allow any user in a given Wi-Fi network, including the attacker, to take control of the coffee machine. The public key would be available to everyone, and the first user to receive it and establish the connection with the coffee maker will be able to control it. Nevertheless, the legitimate user of the coffee machine will at least have a clue that something is going wrong, as during/following? a successful attack they wouldn't be able to communicate with the device. This is not the case with the current software running on the coffee machine.

So we can say that to some degree we understand the vendor logic: the level of risk this issue brings doesn't match the level of complexity of measures that must be implemented in order to eliminate the issue. Besides that, it would be wrong to say that the vendor didn't think about the security of their product at all: as we said earlier, the password is transmitted in protected form, and you have to hold the antenna in a special way.

However, the vulnerability still exists and for a smart criminal it wouldn't be a problem to exploit it to obtain your Wi-Fi password. The situation is interesting: if you are a user of this coffee maker, every time you change the password for your home Wi-Fi network in order to make it more secure, you're actually exposing this new password, because each time you implement a new password you have to set up the coffee machine again. And you would never know whether someone had sniffed your password or not. For some people this may not be an issue, but for others it is most certainly a security problem.

For this reason, we will not disclose the vendor or model so as not to draw unwanted attention to the vulnerable product. However, if you are a user of a smartphone-controlled coffee maker and you're worried about this issue, do not hesitate to contact the vendor and ask them if our findings have something to do with the product that you own, or are planning to purchase.

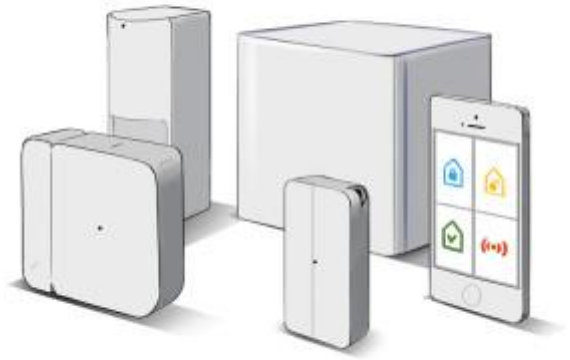
Onto the final chapter of our journey into the insecure world of IoT.

Home security system vs physics

Risk: bypassing security sensors with no alarms

App-controlled home security systems are pretty popular nowadays. The market is full of different products intended to secure your home from physical intrusion. Usually such systems include a hub that is connected to your home network and to your smartphone, and a number of battery-powered sensors that communicate wirelessly with the hub. The sensors are usually door/window contact sensors that would inform the owner if the window or door they guard has been opened; motion sensors; cameras.

When we initially got our hands on a smart home security system we were excited. Previously we'd seen a lot of news about researchers finding severe vulnerabilities in such products, like the research from HP or another awesome piece of research on the insecurity of the ZigBee protocol used by such products, presented at this year's Black Hat. We prepared ourselves for an easy job finding multiple security issues.



But that wasn't the case. The more we looked into the system the better we understood that, from a cyber-security perspective, it is a well-designed device. In order to set up the system, you have to connect the hub directly to your Wi-Fi router, and in order to make the app communicate with the hub, you have to create an account on the vendor's website, provide your phone number and enter the secret pin code that is sent to you via SMS. All communications between the app and the system are routed through the vendor's cloud service and everything is done over https.

When looking at how the hub downloads new versions of firmware, we found that the firmware is not signed, which is a bit of an issue as it potentially allows you to download any firmware onto the device. But at the same time, in order to do so you'd have to know the password and the login of the user account. Also, when on the same network as the security system it is possible to send commands to the hub, but to understand what kind of commands it is possible to send, you'd need to reverse-engineer the hub firmware which is not really security research, but aggressive hacking. We're not aggressive hackers.

So from a software point of view – if you're not intending to hack a device at all costs – the home security system we investigated was secure.

But then we looked at the sensors.

Defeating contact sensors with their own weapon

Intrusion or contact sensors, included in the package, consist of three main parts: the magnet (the part that you put on a door or on the moving part of a window), the radio transmitter, and the magnetic field sensor. It works as follows: the magnet emits a magnetic field and the magnetic field sensor registers it. If the door or window is opened, the sensor will stop registering the magnetic field and will send a notification to the hub, indicating that the door/window is open. But if the magnetic field is there, it will send no alarms, which means that all you need to bypass the sensor is a magnet powerful enough to replace the magnetic field. In our lab we put a magnet close to the sensor, and then we opened the window, got in, closed the window and removed the magnet. No alarms and no surprises.

One could say that it would only work with windows, where you can be lucky enough to locate easily the exact place where the sensor is placed. But magnetic fields are treacherous and they can walk through walls, and the simplest magnetic field detection app for the smartphone will locate a sensor precisely, even if you don't have visual contact. So doors (if they're not made of metal) are vulnerable too. Physics wins!

Motion sensor

Encouraged by an easy victory over contact sensors we moved on to the motion sensor and disassembled it to discover that it was a rather simple infrared sensor that detects the movement of a warm object. This means that if an object is not warm the sensor doesn't care. As we discovered during our experiment, one would only need to put on a coat, glasses, a hat and/or a mask in order to become invisible to the sensor. Physics wins again!

Protection strategies

The bad news is that magnetic field sensor-based devices and low quality infrared motion sensors are used not only by the home security system we investigated. They're pretty standard sensors which can be found in a number of other similar products. Just search the IoT e-shops and you'll see for yourself. There is more bad news: it is impossible to fix the issue with a firmware update. The problem is in the technology itself.

The good news is that it is possible to protect yourself from the burglars who didn't bunk off Physics in school. The basic rules here are as follows:

1. Do not rely only on contact sensors when protecting your home if you are using a system of the kind described above. Smart home security system vendors usually offer additional devices, like motion- and audio-sensing cameras, which are impossible to bypass with magnets. So it would be wise to supplement the contact

sensors with some smart cameras even though it may cost more. Using contact sensors alone will turn your home security system into what is essentially a high-tech ‘toy’ security system.

2. If you’re using infrared motion sensors, try to put them in front of a radiator in rooms a burglar will have to walk through, should they make their way into your home. In this case the intruder, no matter what clothes they are wearing, will overshadow the radiator and the sensor will notice the change and report it to your smartphone.

Conclusions

Based on what we discovered during our brief experiment, vendors are doing their best not to forget about the cyber-security of the devices they’re producing, which is good. Nevertheless, any connected, app-controlled device that is usually called an IoT device is almost certain to have at least one security issue. However, the probability that they will be critical is not that high.

At the same time, the low severity of such security issues doesn’t guarantee that they won’t be used in an attack. At the beginning of this article we promised to describe how the safe and funny “rickrolling” vulnerability could be used in a dangerous attack. Here it is.

Just imagine that one day a TV with a Chromecast device connected to it, both belonging to an inexperienced user, starts showing error messages which report that, in order to fix this issue, the user has to reset their Wi-Fi router to factory settings. That means the user would have to reconnect all their devices, including their Wi-Fi-enabled coffee machine. The user resets the router and reconnects all the devices. After that the Chromecast works normally again as do all the other devices in the network. What the user doesn’t notice is that someone new has connected to the router, and then jumped to the baby monitor camera or other connected devices, ones that have no critical vulnerabilities but several non-critical ones.

From an economic perspective it is still unclear why cybercriminals would attack connected home devices. But as the market of the Internet of Things takes off, and technologies are being popularized and standardized, it is only a matter of time

before black hats find a way to monetize an IoT attack. Ransomware is obviously a possible way to go, but it's certainly not the only one.

Besides that, cybercriminals are not the only ones who might become interested in IoT. For instance, this summer the Russian Ministry of Interior Affairs ordered (RU) to research possible ways of collecting forensic data from devices built with the use of smart technologies. And the Canadian military recently published a procurement request for a contractor that can "find vulnerabilities and security measures" for cars and will "develop and demonstrate exploits".

This doesn't mean that people should avoid using the IoT because of all the risks. The safe option is to choose wisely: consider what IoT device or system you want, what you plan to use it for and where.

Here is the list of suggestions from Kaspersky Lab:

1. Before buying an IoT device, search the Internet for news of any vulnerabilities. The Internet of Things is a very hot topic now, and a lot of researchers are doing a great job finding security issues in products of this kind: from baby monitors to app controlled rifles. It is likely that the device you are going to purchase has been already examined by security researchers and it is possible to find out whether the issues found in the device have been patched.
2. It is not always a great idea to buy the most recent products released on the market. Along with the standard bugs you get in new products, recently-launched devices might contain security issues that haven't yet been discovered by security researchers. The best choice is to buy products that have already experienced several software updates.
3. When choosing what part of your life you're going to make a little bit smarter, consider the security risks. If your home is the place where you store many items of material value, it would probably be a good idea to choose a professional alarm system that will replace or complement your existing app-controlled home alarm system; or set-up the existing system in such a way that any potential vulnerabilities would not affect its operation. Also, when choosing the device that will collect information about your personal life and the lives of your family, like a baby monitor, maybe it would be wise to choose the simplest RF-model, capable only of transmitting an audio signal, and without Internet connectivity. If that is not an option, than follow our first piece of advice – choose wisely!

As for the vendors of IoT-devices, we have only one, but important suggestion: to collaborate with the security community when creating new products and improving old ones. There are initiatives like Builditsecure.ly or OWASP Internet of Things project that could actually help to build an awesome connected device with no serious security issues. At Kaspersky Lab, we will also continue our research to get more information about connected devices and to find out how to protect people against the threats that such devices pose.