THE STATE OF IOT SECURITY

It is time for action.

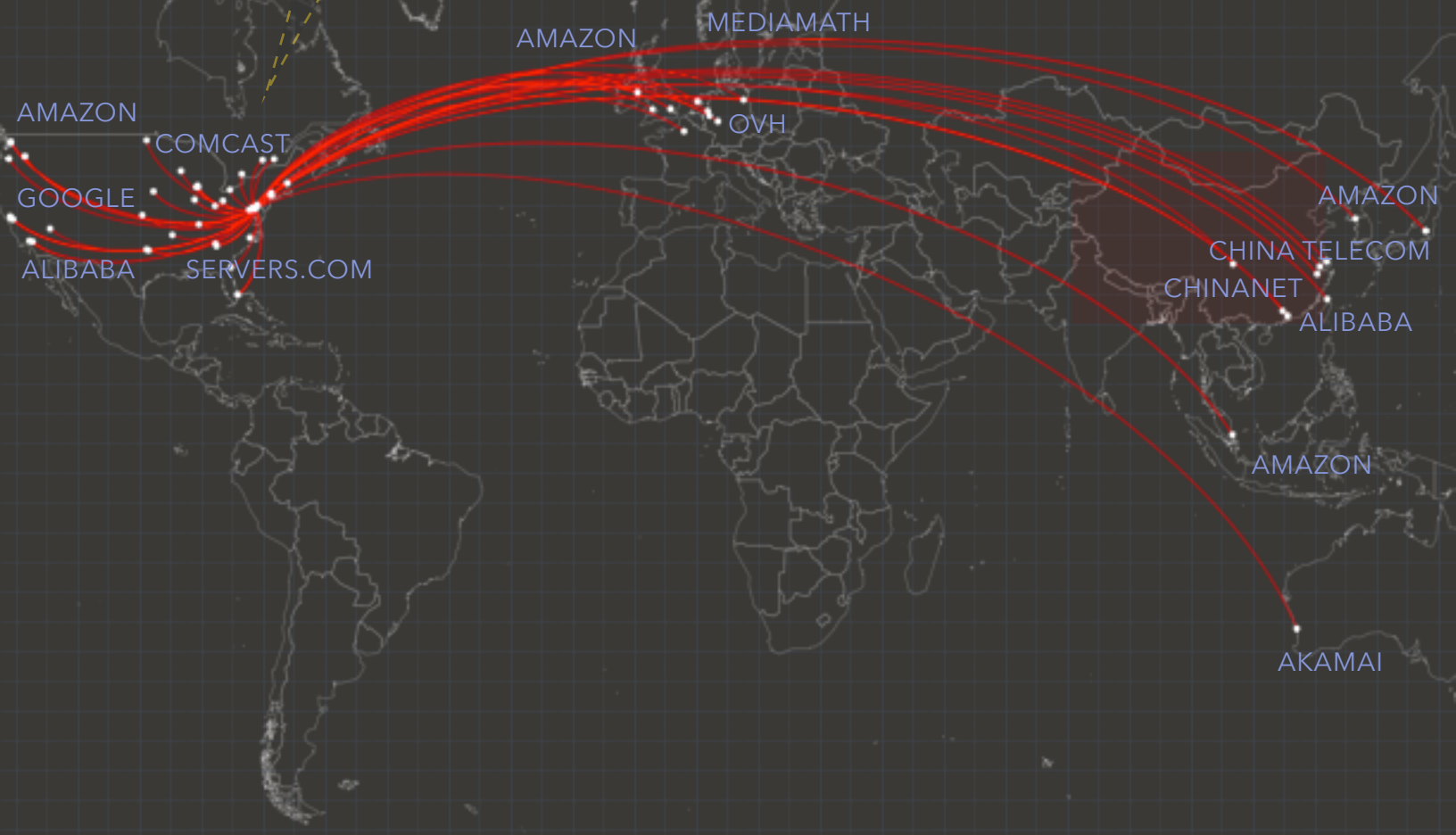
dark3

THESTATEOFIOTSECURITY.COM

Schedule A

The Impact of IoT

By installing just 12 IoT devices purchased off-the-shelf from well-known retailers, our personal information and other data began spreading across the globe.



Disclaimers

No laws were broken in the development of this report and no networks were accessed without the express permission of the owners.

This entire report was written and designed by the technical team at Dark Cubed. This report was not composed or graphically designed by a marketing or advertising firm. As such, we accept full responsibility for any typos or errors. If any of our statements or findings are found to be in error, we will swiftly correct or retract such statements after confirming the error and will be certain to publicly accept responsibility for any such errors.

China can track you through your light bulb. Do you care?

According to leading global research and advisory firm Gartner, there were an estimated 8.4 billion Internet of Things (IoT) devices in use worldwide in 2017. That number is expected to grow to over 20 billion devices by 2020. Within the security community, it is widely understood that while many of these devices are not secure, most people remain unconcerned about this fact.

As security experts, we understand the fatigue associated with discussions on the security of IoT devices, we feel the same way. However, we had our interest piqued in this project by the observation that our customers were being attacked by rogue IoT devices and decided to look into this matter ourselves.

Our tests were not complex, esoteric hacking, rather they were simple, boring security tests that anyone even considering security would have performed. We performed these tests through a rigorous, exhaustive review of each individual device to collect hard data on the state of security for these devices, the results of which we are excited to share in this report. Our findings are the result of analyzing over 1.25 million communications to more than 3,000 external servers from 12 off-the-shelf IoT devices.

What we found, on one hand, was not surprising. Many of these devices are not secure. Much of the associated infrastructure is not secure. Several of the Android applications are borderline dangerous.

However, what was surprising was the fact that some of these devices, such as the IoT light bulb, were so insecure that it is beyond what could be considered a mistake. We found that the extent to which the manufacturers and infrastructure associated with these devices communicate with, or is related to, China is shocking and has significant national security implications.

It is not all bad news though. Some of the devices, applications, and infrastructures are secure, are not more expensive than the insecure ones, and do not communicate with servers in China. Unfortunately, consumers have no ability to differentiate between the safe and the dangerous devices given the lack of focus on security by retailers.

We are excited to share our findings with the broader security community and look forward to continuing the discussion on securing the future of IoT.

Key Findings Up Front

Several of the devices reviewed were painfully insecure.
While some of the devices were well implemented, it was obvious with some of the IoT devices we reviewed that neither the company, its manufacturer, nor its platform provider have ever seriously considered security a priority.

A few of the associated Android applications were terrifying.
When you have to open up a line of communications to China and enable real-time location sharing just to dim a lightbulb, you should be concerned. We identified a number of serious systemic security flaws that worry us about the future of IoT.

There are a number of IoT companies but some do not seem to care about security.
IoT is a fast-growing market, however what we found is not just that these companies did not catch all of the security flaws, rather we found that the manufacturers and retailers are likely not even considering security at all. This has to change today if we have any hope of being secure tomorrow.

There is reason to be concerned about the role of China in IoT.
There is a mountain of research related to China's perspective on compromising supply chains and critical infrastructure to gain a strategic advantage. With most IoT devices being manufactured in China, we need to think about mitigating this threat by requiring secure and trusted communications before it is too late.

The use of cloud-based infrastructure does not mitigate security threats.
A majority of the infrastructure we observed is located within Amazon Web Services, but much of it is not secure. Just because these companies are using cloud infrastructure from well-known companies, the security risk is not reduced.

Patching will not fix the systemic issues we found.
If the response to our findings is a simple, "we will fix those issues," then we have failed. The problem is not the existence of the security flaws, rather the fact that there are systemic issues within manufacturering and retail where security is not a consideration, it has to be.

dark3

OUR RECOMMENDATIONS

Consumers must demand protection.
It is right for consumers to expect that retailers watch out for their best interests. This problem is no different from unsafe toys, expired foods, or protecting customers from items made with toxic chemicals. While consumers may have a difficult time determining if a device is secure, they can demand that the retailer considers security of IoT devices before placing them on their shelves.

Retailers have to take responsibility.
Consumers have no means to assess whether a device is secure or not and manufacturers apparently have no incentive to secure their devices. Therefore, it is the responsibility of retailers to sell safe and secure IoT devices to consumers.

Government should take action.
While we do not necessarily think regulation is the answer for most problems, we are clearly on the edge of a National Security crisis with respect to the role of China in IoT devices. The U.S. Government must act to ensure the safety and security of IoT devices and to ensure that the data of its citizens is protected.

Why we wrote this report

The Dark Cubed team is made up of security geeks that are passionate about protecting the underserved. We are focused on helping small and midsized companies implement enterprise-grade cyber security capabilities at a price point and level of complexity that works for their business. In the course of our day-to-day business, we are seeing an increasing number of attacks conducted by armies of Internet of Things (IoT) devices and can only assume this is a fast-growing trend. According to Gartner, there were around 8.4 billion IoT devices, going up to over 20 billion devices by 2020[1]. If we are concerned with attacks and the security of these devices now, wait until we have more than twice as many devices in the world.

What is IoT?
*The Internet of Things, commonly abbreviated as IoT, refers to the connection of devices (other than typical fare such as computers and smartphones) to the Internet. Cars, kitchen appliances, and even heart monitors can all be connected through the IoT. And as the Internet of Things grows in the next few years, more devices will join that list.**

The trigger for performing this research project came about a year ago from a small posting we saw on Twitter involving a list of over 8,000 default usernames and passwords tied to IoT devices in people's houses. We conducted a research project on that dataset and quickly discovered a large percentage of those devices had targeted our customers. After letting those thoughts stew for about a year (and while we were building our new software-as-a-service infrastructure), we decided it was time to act. This report is the result of countless hours of research and analysis by the team at Dark Cubed and was made possible by the technology that we have developed to protect our customers.

Approach and Methodology

We have read many, many, MANY briefings, reports, and news articles on the insecurity of IoT devices. We knew up front that we did not want to do another report on how you can take these devices apart and hack them, or even show how you can reverse engineer the software to make bad things happen. These are security risks that are incredibly hard to mitigate and manage, and frankly, make the security discussion harder because they are so difficult to prevent.

We decided we would take the approach of looking at the communications coming in and out of these devices and their associated Android applications to see what we could find.

We knew we would not have the time or energy to go down every rabbit hole on weaknesses we found, so we attempted to keep focused on providing a clear understanding against a simple question: Given how these devices communicate, can we gain visibility into the security mindset of the manufacturers?

---

*Definition of the Internet of Things (IoT) source from an article published on May 10th, 2018 by Andrew Meola in on businessinsider.com, found online at: https://www.businessinsider.com/internet-of-things-definition

[1] Leading the Iot: Gartner Insights on How to Lead In A Connected World, Hung, Mark, Gartner, 2017, found online at: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

We include all of the extensive details of our analysis in a separate Technical Volume of this report, which represents almost 200 pages of the fine details of what we found. We will be sharing this with the technical community soon but wanted to share our findings at a higher level for a much wider audience now. Just know that everything we state in this report can be backed up by raw data and rigorous analysis. At a high level this analysis included the following activities:

- a manual review of the privacy policy of each device to understand how the company protects customer data and to whom it is shared with,
- monitoring and scoring all traffic using advanced threat intelligence analytics in the Dark Cubed platform,
- logging all traffic and analyzing communication patterns,
- collecting full packet data for manual reviews of communications,
- executing a man-in-the-middle attack to understand what someone outside of your network could see, and,
- performing automated and manual analyses of the associated Android applications.

An Introduction to Internet of Things (IoT) Devices

If you already understand how IoT devices function, feel free to skip to the next section, but since we are focused on the security of these devices, a quick primer on how they function is an important piece of background. We put together the graphic below to show you just how much goes into a simple IoT light bulb.

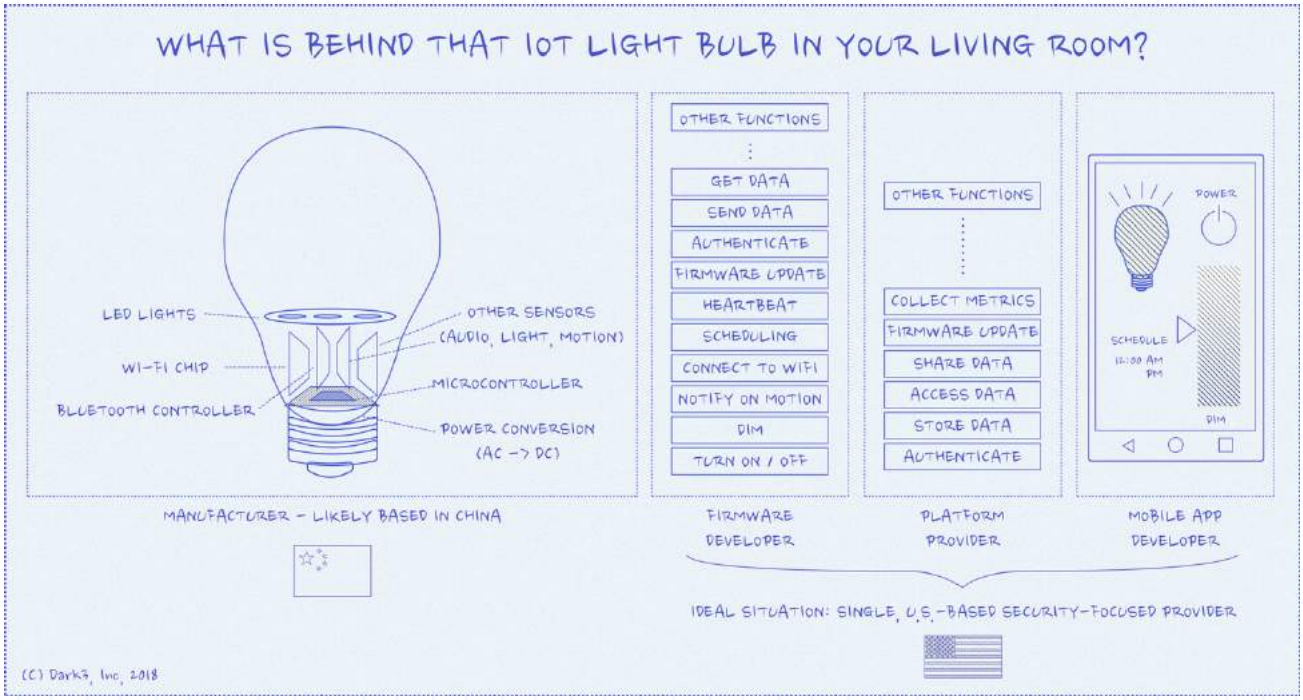


Figure 1: Overview of what is behind that IoT light bulb in your living room

As you can see from the graphic on the previous page, we divide the activity associated with the light bulb into several groups. First, we have the manufacturer. In most of the devices that we have seen, these devices are manufactured in China and then sold to companies which brand them as their own product. In most cases, the components of the bulb actually have unique manfacturers as well, so one manufacturer may provide WI-FI controllers that are used on many different IoT devices. These devices are manufactured with a microcontroller, a small computer that controls the functionality based on firmware (software) that is written for it. There can be many versions of firmware for a single hardware device.

The firmware also controls communcations to the provider of the storage platform. In this study, we saw a number of platform providers such as MeShare.com, Pepper, Tuya, and others. The platform provider manages the distribution and storage of information and grants access to the devices to interact with data that might be stored on the platform.

The last piece is a mobile application that is developed to interact with both the platform and the IoT device to implement functionality.

In some cases, all of these parts and pieces are developed by the same company, in others, different companies can manage each component. To further complicate things, in some cases, there may be a number of different mobile applications that will all interact with the same IoT device to allow users to manage devices from different companies in a single interface.

The final component has to do with how communications occurs between the device, the infrastructure and the Android phone. This can happen over Wi-Fi or cellular data. For some of the devices we reviewed, communciations happened directly between the mobile phone and the device when they were on the same network, but for others, communiations always occured through the remote infrastructure.

From a security perspective, we are mostly concerned about the firmware developers, the platform provider, and application development. We are less concerned about the device manufacturers due to the fact that the software running on the hardware controls the functionality when it comes to consumer-grade IoT devices. With this in mind, the best-case scenario is for the device to leverage a single trusted, preferably U.S.-based, provider for all three of the key functions: firmware, platform, and mobile application. This provider would idealy focus on security as a key tenant of its business model and would embrace openness and transparency with consumers and retailers alike.

Devices Reviewed

To select our devices, we simply walked the aisles of Walmart, Best Buy, MicroCenter, and browsed devices on Amazon. We tried to get a mix of cameras, outlets, and we even grabbed a light bulb. The table below lists the devices we ended up testing.

Manufacturer	Model	Model Number
iHome	SmartPlug	ISP6WC
Merkury	Smart WiFi Outdoor Plug	MI-OW101-101W
Merkury	Smart WiFi Plug	MI-WW105-199W
Merkury	Smart WiFi LED Bulb	MI-BW902-999W
Merkury	Smart WiFi Camera	MI-CW007-199W
Momentum	Axel Camera	MOCAM-720-01
Oco	Oco 1 WiFi Camera	CO-14US
Practecol	Guardzilla Security System	GZ502B
TP-Link	Kasa HS105 Smart Plug	HS105
Vivitar	Smart Security Camera	IPC113-WHT
Wyze	WyzeCam	WYZECP1
Zmodo	Mini WiFi Camera	ZM-SH75D001-WA

Table 1: Devices selected for analysis

Figure 2: A lineup of the twelve devices we reviewed

Key Findings

Finding #1: Several of the devices reviewed were painfully insecure.

A number of the devices we reviewed appeared to keep third-party communications to a minimum, followed basic security principles, and produced a product that we would not mind gifting to our friends and family. Namely, the iHome Smart Outlet, the Momentum Axel Camera, and the TP-Link Kasa Smart Outlet were all well developed, secure, and straighforward devices with no identified communications of concern.

Several of the devices, however, have been implemented on platforms that either (A) do not fully utilize encryption for the transmission of information or (B) would allow anyone to bypass the encryption due to poor implementation. We are certainly concerned about the devices themselves, however we strongly suspect that the security issues we found are representative of the fact that these companies have not considered security important enough to even conduct a single security review of these devices. No security-minded individual at these companies would allow some of these devices out the door in their current state. For example, the Merkury devices all use a very insecure implementation of a technology coined pub/sub (MQTT for the technical folks). With this technology, the Merkury devices monitor a specific message queue for instructions, such as turning on and off. These instructions are dropped into that queue by the Android application. By merely observing unencrypted traffic on our network, we were able to get full visibility into the names of the queues used by each device, as well as the username and password necessary to access those queues. With this information, a simple, five-line computer script would allow anyone to know every time that you turn a light or outlet on and off. It is also possible that with some technical proficiency a malicious individual could also issue instructions to manipulate those devices without the homeowner having any way to stop it without unplugging the devices.

The Guardzilla and Zmodo devices are also excellent examples of devices with scary security issues. Neither of these devices was confirming that the encryption certificate for encrypted communications was valid. With a quick and free implementation of a man-in-the-middle attack, we were able to see the images going from these devices to the cloud. Even worse, anyone between the user's house and the cloud servers could do the same. There is no excuse for not preventing this from happening. The only explanation is that these companies have never actually performed a security review on their devices. We have many more examples of these weaknesses in our soon-to-be-released Technical Volume of this report.

Finding #2: A few of the associated Android applications were terrifying.

It is common for us to hear someone say "big deal" when talking about the security of a light bulb. For example, the Merkury light bulb does very little, it does not have a camera and does not record audio. So, it is easy to assume there is minimal risk here. However, to turn the Merkury bulb on and off, you need to install the Geeni Android Application on your phone. Once you install this app, it gives you access to a specific set of explicit functions that control the light bulb, including dimming the bulb, turning it on and off, and scheduling when the bulb should be turned on and off automatically.

Figure 4: The Merkury Smart Light Bulb

But, that is not all the app can do. While we did not do a detailed vulnerability analysis of the Android application, what we found was terrifying. The app itself requires a significant number of permissions such as knowing your location at all times, recording audio, and reading and writing to external storage on your phone. It also includes the SYSTEM_ALERT_WINDOW permission which Google advises, "Very few apps should use this permission; these windows are intended for system-level interaction with the user." This permission may seem like an innocuous thing, but there are some interesting write-ups around how using such functionality could allow an application developer to actually steal data from other applications, compromise passwords, or even enable the download of malware onto the device. Now we certainly aren't suggesting that the developers of the Geeni application have considered this, but it is something that makes us nervous.

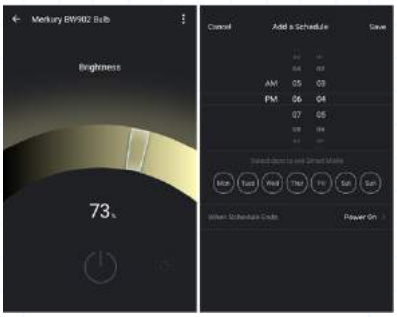


Figure 3: Light bulb functionality in the Geeni Application

Further, this application has hard coded links to about 40 third-party websites within the application code to include both U.S. and China-based entities such as Alibaba, Taobao, QQ, Facebook, Twitter, and Weibo to name a few. It is highly likely that this application does a significant amount of mining of personal data for advertising purposes. During our testing, this application also performed numerous communications to web servers in China, Hong Kong, in addition to U.S.-based servers. Just by dimming your light bulb, you are taking on an incredible amount of risk due to security issues and the leakage of personal information with the application. So, how do you feel about that simple little light bulb now?

Several of the other Android applications were also vulnerable to man-in-the-middle attacks and had other issues, such as a hardcoded password within the Guardzilla application. A summary of our finding related to the Android applications is included in the table below.

	Normal Permissions	Dangerous Permissions	Special Permissions	Not For Third Party Permissions	Hardcoded Password	Third-Party Domains	Vulnerable to Man-In-The-Middle	Access to Location Data
Guardzilla	9	8	0	4	!	11		●
iHome	5	2	0	0		11		●
MERKURY	7	6	1	0		40	●	●
momentum	7	5	0	0		12		
oCo	5	6	0	0		10		●
tp-link	8	4	3	0		17	●	●
VIVITAR	10	11	1	2		36	●	●
WYZE CAM	7	3	0	1		15		
zmodo	17	7	1	4		20	●	

Figure 5: Overview of Android application findings by device

The table above shows the number of permissions we found in each category as defined by the Android developers guide. It is important to note that it is typical for the average user tends to just accept permissions associated with an application upon install and to never consider them again.

We also indicate that we found hardcoded password within the Guardzilla application. The third-party domains number refers to the number of unique third-party domains we found hardcoded into the application. We also represent whether the application was fully or partially vulnerable to a man-in-the-middle attack. Finally, we show whether the application requested access to the user's location as a required permission for functionality.

For a little more detail on the permissions requested by each device, we have included this information in the table below. In this table we characterized the different types of permissions as those that we consider to be relatively safe and normal and those that we see as dangerous or concerning.

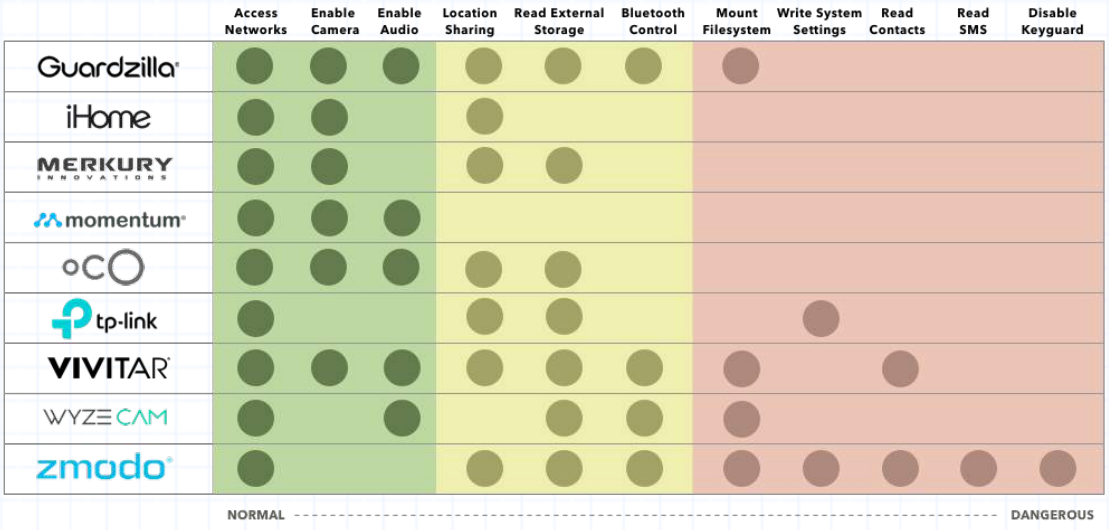


Figure 6: Summary of Android application permissions

It is important to note that the existence of a dangerous permission does not necessarily mean that the application is actually using the functionality. In some cases, it is possible that the inclusion of a specific permission is a mistake or an oversight. However, it is concerning that once the user grants permission to an application on Android, the application, or future updates of the application, can use those permissions without requesting permission again.

Finally, we also want to clearly state that we only tested the Android versions of these applications. Given Apple's historic focus on more tightly controlling permissions and reviewing applications from a security perspective, it is certainly possible that some of the issue we found with respect to permissions do not exist within the iOS version of the applications.

Finding #3: There are a large number of IoT companies and startups, but some obviously do not care about security, and neither do the retailers.

While relatively few in number, the devices we reviewed represent a strong sampling of the IoT devices we expect consumers to be purchasing at retail locations given their prominence on the display shelves as shown in the image below.

Figure 7: The TP-Link, iHome, and Merkury Devices on the Shelf at Walmart

We observed a surpisingly large variation in how these companies consider security. Some companies had glaring security problems in both the application and their hardware device(s).

Given what we found it is clear that some companies have not seriously considered security to be a part of their business model. When we see gaps such as the sending of sensitive information in an unencrypted form or obvious weaknesses in how the company implemented encryption, we have to assume that some of these devices have never undergone a single security review.

For example, pretty much every message coming in and out of the Zmodo camera and the Android application was implemented in such a manner that we could intercept all communications easily; even if the communication was encrypted. Anyone could do this at home with a few simple tools. *This security weakness gave us full access to sensitive information sent to and from the Android application such as birthdates, e-mail addresses, phone numbers as well as the ability to view every image and video coming out of the device.*


```
{
  "result":"ok",
  "data":{
     "id":"12930938",
     "username":"allyouriot",
     "email":"allyouriot@gmail.com",
     "password":"ae3e02685469d234b49b602b67cbed2b",
     "create_time":"1532124888",
     "firstname":"john",
     "lastname":"smoth",
     "nickname":"allyouriot2",
     "photoid":"",
     "gender":"0",
     "birthday":"2017-09-12",
     "country":"United States",
     "location_level1":"",
     "location_level2":"",
     "location_level3":"",
     "zip_code":null,
     "showdevice":"0",
     "about":"",
     "timestamp1":"1532723626560",
     "timestamp2":"1532723626560",
     "flag":"1",
     "account_id":"",
     "account_type":"0",
     "photo_url":"",
     "phone_number":null,
     "phone_region":null,
     "company_id":"0",
     "platform":"2",
     "own_idc":"1"
  },
  "addition":""
}
```


Figure 8: Personal information leaked from the Zmodo Android Application

Further, some of the devices are built to interact with third-party platforms such as the Momentum and the Merkury devices, but the implementation of these platforms is anything but standard. The Momentum devices and Android Application appear to be related to a platform company known as Pepper which has an infrastructure in Amazon Web Services and the device, the data communications, and the application appear to be well locked down. The Merkury devices are associated with a platform provider named Tuya. The Merkury devices and the required "Geeni" Android application were found to have several security flaws. Further, while the Merkury smart outlets and light bulbs had no communications outside of their AWS infrastructure, the smart camera has a significant amount of interactions with servers connected to Alibaba in China. Even worse, the Geeni application associated with these devices had some significant issues that are concerning, such as overly broad permissions and what we deem to be an excessive number of links to advertising and tracking sites both in the United States and China.

To sum up our findings, the table on the following page presents a view of our observations on the hardware devices and the associated Android applications.

	Device Type	Headquarters	Other Countries Receiving Data (Non-AWS Servers)	Access to Location Data	Vulnerable to Man-In-The-Middle	Third-Party Domains in Android Application	Observe or Manipulate Communications	Privacy Policy
Guardzilla	Security System	US	CN	●	●	11	🔍	😐
iHome	Smart Outlet	US		●		11		🙂
MERKURY INNOVATIONS	Camera, Smart Plug, and Smart Light Bulb	US	CN	●	●	40	🔍	☹
momentum	Camera	US				12		🙂
oCo	Camera	US	DE	●		10		🙂
tp-link	Smart Outlet	CN	US	●	○	17		🙂
VIVITAR	Camera	US	CN HK	●	●	36		☹
WYZE CAM	Camera	US			●	15		🙂
zmodo	Camera	CN	US		●	20	🔍	😐

Figure 9: Summary of all findings by device

As shown on the previous page, we see most of the devices claim to have a U.S.-based headquarters, but a few were observed sending data to other counties such as China, Hong Kong, and Germany. For example, we observed the Guardzilla, Vivitar, and Merkury devices communicating with servers in China associated with Alibaba and China Telecom, while the Oco camera communicated with servers associated with OVH Hosting in Germany.

We indicate whether the associated Android application required access to location data and whether we were able to gather data using a man-in-the-middle attack against either the device or the application. The number represents the number of unique third-party domains we found hardcoded into the Android application. We also show whether we were able to observe or manipulate communications between the device and its infrastructure. For this item, we have three indicated devices:

- for the Guardzilla device we were able to trigger false alarms by simply visiting a URL in our browser,
- on the Merkury devices we were able to observe all actions taken to turn on and off the light bulb and smart outlets and were also able to observe a number of communications associated with the Merkury camera, and,
- for the Zmodo Camera, we were able to observe every communication made to and from the camera, to include images and video.

Finally, we indicate our qualitative perspective on the Privacy Policy for each company. Well, written and focused policy statements received a happy face, while those policies that were overly broad and non-restrictive received a sad face.

Finding #4: There is reason to be concerned about the role of China in IoT.

There is cause for alarm with the relationship between China, Chinese Companies, and the billions of devices in consumers households. It is correct to say that just because a company operates in China does not make it an evil company. However, the relationship between business and Government in China is different than in other countries. The U.S. Intelligence Community's February 2018 Worldwide Threat Assessment[2] clearly states, "China will continue to use cyber espionage and bolster cyber attack capabilities to support national security priorities." While broad, when you combine this statement with extensive documentation of China's attempts to compromise supply chains and gain access to information, influence, and control, the Internet of Things is an obvious target.

There remain significant concerns from the U.S. Government and other Foreign governments around the ongoing efforts of China to use telecommunications companies such as Huawei and ZTE to gain access to global infrastructure to enable China's strategic priorities. This concern is so broad that in February of 2018 six key leaders of the U.S. Intelligence committee testified to the Senate Intelligence Committee against buying products from or using services provided by

[2] Statement for The Record, Worldwide Threat Assessment of the U.S. Intelligence Community, Coats, Daneil R., February 13th, 2018, found online at: https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

Huawei or ZTE. FBI Director Christopher Wray went so far as to state the following, "We're deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks. That provides the capacity to exert pressure or control over our telecommunications infrastructure. It provides the capacity to modify or steal information maliciously. And it provides the capacity to conduct undetected espionage."[3]

We do not have the time to go much deeper into the background on concerns associated with China in this report, however, based on our extensive experience in this area we can say a few things conclusively about IT supply chains, China, and IoT.

1) China will continue to manufacture most IoT devices in the coming years due to issues of labor and the cost of materials
2) China can compromise the IoT supply chain due to the relationship between China, Chinese State-Owned enterprises, and the control over which China has on other companies operating in China.
3) No company with facilities in mainland China can operate completely independent of the Chinese Government.

Given these three facts, and the explosion of IoT devices in the coming years, we found several items of significant concern in this study.

1) A number of the IoT devices and their Android applications were observed sending data to China in a format that we could not decrypt. These communications do not inherently imply anything malicious is happening. However, they do create a protected communications channel from U.S.-based devices back to mainland China.
2) A number of these devices have direct connections to Chinese-based companies such as Alibaba, Tuya, and other entities on China Telecom. Even if these devices are not at risk now, due to the relationship between the Chinese Government and Chinese companies, it is conceivable that if China wanted to use these devices for malicious means, it would be easy to accomplish.
3) Some of the companies publicly state that their headquarters are in China. For example, the Zmodo and the TP-Link devices both come from companies that proudly claim their headquarters in Shenzhen, China.
4) Some companies had less apparent ties to China, but they are there. For example, the Vivitar device had regular communications with Alibaba servers; however, there is no obvious relationship between Vivitar and Alibaba. The Wyze camera appears to come out of a hip startup in Seattle, Washington; however, the name of their Android application points to a Chinese company that is marketing the same device in China. There are numerous examples of strange connections to China for many of the products we reviewed as explained in the technical volume.

[3] Six top US intelligence chiefs caution against buying Huawei phones, Salinas, Sara, February 13th, 2018, CNBC.com, found online at: https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html

Finding #5: The Use of Cloud Infrastructure does not mitigate security threats.

Some companies claim that they are on AWS or another U.S.-based cloud platform, making their platform secure. This statement is patently false, and we can prove it. It is essential to differentiate between using a secure platform such as the Amazon IOT or Google's IOT platforms and using a web server on Amazon Web Services. Amazon has no responsibility, nor should they, to secure infrastructure housed within AWS on a virtual server.

For example, we reviewed Merkury's (Tuya's) implementation of the publication / subscribe infrastructure used to turn on and off light bulbs and outlets. Not only were the communications being passed in the clear, but the username and passwords were as well. As a result, anyone could intercept the interactions between your phone and your IoT device to gain visibility into your comings and goings. It would be trivial for Merkury/Tuya to implement security for these communications, but they have not done so. So, while it is true that the server is within AWS, it is indeed not secure. Many of the security flaws we found were related to services communicating to servers housed within AWS. We do not hold Amazon accountable for this as they are providing the servers and it is up to the user to secure those servers appropriately.

Another example is with the Vivitar camera. This camera was observed sending data to both Amazon Web Services and Alibaba networks. While the infrastructure associated with the devices we reviewed only communicated with a small number of services such as DNS, HTTP, and HTTPS, this device was observed communicating with a significantly higher volume of ports, potentially resulting in less ability to manage security. Further, when looking at open ports on the infrastructure this device communicated with, we saw an abnormally high volume of open ports, resulting in a complicated, very likely hard to manage infrastructure.

Finding #6: Patching will not fix the systemic issues we found.

While companies can undoubtedly patch their devices to fix many of the issues we found, the problem is much more severe: many product companies do not care about security and only act when outsiders find issues. This reactive approach does not work, security must be proactive.

The systemic issues must be fixed if we have any hope of security and privacy. Said another way, if any one of the companies covered in this report take our report and patch the issues we found, they still will not be secure. Security requires a culture and commitment to protecting the privacy and security of consumers. We would have to see significant restructuring and realignment in these companies focused on making security a priority to feel comfortable even considering the use of some of these products again in the future.

Further, as previously stated, we purchased these devices from WalMart, Best Buy, Amazon, and MicroCenter. Given some of the glaring security flaws in these devices, it is clear that retail buyers are not being directed to consider security as part of their purchasing decisions. Buyers at retail locations would not consider buying dangerous toys, spoiled food, or counterfeit drugs, but horribly insecure IoT devices? No problem! What's even worse, we assert that if buyers DID consider security in some form or fashion, they could protect consumers from significant

security and privacy risks AND prices are unlikely to go up. To say that another way, several of the devices, to include the TP-Link, iHome, and Momentum devices were relatively secure with no apparent security flaws, yet those devices were no more expensive than the most flawed devices. For example, the Zmodo device was the scariest of all the cameras we investigated, yet at $34.99 from Walmart, it is not much cheaper than the more secure Momentum camera which comes in at $36.88. Is the privacy of your sleeping children worth an additional $1.89? More importantly, do consumers have any way of knowing the drastic difference between these two cameras if the retailer does not look out for them?

Summary

In summary, we were shocked by our findings in this study. Coming from security experts that expect things to be insecure, this is saying something. While we certainly expected to find vulnerabilities and weaknesses, the obvious nature of the security flaws we found was surprising. These flaws were so blatent and obvious that it is more than just a mistake, it is a systemic issue that needs to be addressed.

When looking at devices like the Zmodo or Vivitar cameras, a combination of concerns piled up to make the devices unusable to anyone who considers security or privacy to be a priority. The Merkury devices, which are stocked heavily in the aisles U.S. retail store also have a surprising number of issues. We found these devices made sensitive communications without encryption, were susceptible to man-in-the-middle attacks and had a staggering volume of third-party domains referenced in the Android application. Further, we found that the role of China in IoT is very concerning with respect to the access that China is gaining into sensors placed in the homes and mobile devices of unwitting consumers and the data they are able to collect as a result.

Based on our findings we came away with three key recommendations that we would like to present to the community at large for debate.

1) **Consumers must demand protection.** First and foremost, we found that while these blatant security flaws exist, consumers have no ability to base purchasing decisions due to the lack of concern for this issue by retailers. A consumer can not buy an unsafe toy, milk that has been expired for months, or toys made out of asbestos, but they can buy an IoT camera that will allow strangers to watch their kids sleep at night. This is unacceptable, and consumers must demand that the retailers protect them from unsafe IoT devices.
2) **Retailers have to take responsibility.** It is clear that some manufacturers and platform providers do not care at all about security. It is the responsibility of retailers to identify these bad actors and either demand action or buy from manufacturers and platform providers that do care. Based on our analysis, this process would not place a significant financial burden on retailers and significant gains in security could be achieved quickly. We are happy to provide our methodology and results to retailers to be used in

developing their own processes if that would help. Based on what we saw, we could quickly and easily assess any IoT device on the shelves of retailers in a repeatable, reliable fashion that would not slow down the process used by buyers to stock their shelves. This is not hard, it just is not being done yet.

3) **Government should be involved.** We tend to think that government regulation against technology tends to slow down innovation and is not necessarily the solution to all problems, however, there is a need for the Government to act in some form or fashion. The United States (and other countries for that matter) is going to wake up in the coming years and realize that China has established an irreversible foothold on sensors monitoring, and data belonging to, every American. China's ability to manipulate and interact with this sensor grid at will is a clear and present danger that must be addressed. This is an area of economic and national security risk is where only the Government has the authority to demand protection for its citizens.

We welcome further discussion and dialog on this topic and look forward to publishing more of our findings as we have the time to do so. In the meantime, thank you for reading this report, and we hope you IoT safely from here on out!

About Dark Cubed

Dark Cubed is a different kind of cyber security company.

We come from a diverse set of backgrounds with experience in large and small companies, the U.S. Government, the military, and National Laboratories. We have protected White House networks, helped to secure the United States information and communication technology supply chain, and helped build massive multi-billion-dollar programs focused on protection the U.S. Government and critical infrastructure from highly sophisticated nation-state threat actors. Many of our peers are drawn to create cyber security companies that focus on finding and stopping the hardest, most sophisticated threats, driving them to work with the largest enterprises in the world.

We went the other direction.

Our passion is with the other 99% of businesses. The doctor's offices, the financial advisors, the law firms, the small energy co-op in the Midwest. We believe that if security is not designed from the ground up to work for small and midsized businesses, then security will never be affordable and accessible for these companies. Even worse, if these companies are not secure, none of us ever will be.

We started Dark Cubed to rethink the delivery and deployment of cyber security capabilities to small and midsized companies, and are humbled to have experienced strong traction and success to date. As members of the broader security community, we feel it is important to give back and contribute thoughtful reports and analysis back into the realm of public discourse. This report represents such an attempt, and we are honored to have the opportunity to share some of our thoughts and ideas with anyone that is willing to read this report.

Report Authors

Vince Crisler

Vince is the CEO and Founder of Dark Cubed. He is the former Chief Information Security Officer at the White House and a proud Veteran of the U.S. Air Force with service at the Pentagon, the White House and Ramstein Air Base in Germany. Vince also supported the Department of Homeland Security in their National Cybersecurity Programs for over five years.

Bryan Richardson

Bryan is the CTO of Dark Cubed and built the Dark Cubed platform from scratch. He formerly served for over 10 years at Sandia National Laboratories performing extensive research, development, and engineering in the field of cyber security and control systems security. Bryan also supported the National Cybersecurity Programs at DHS for several years prior to joining Dark Cubed.

John DiGerolamo

John is a senior analyst and engineer at Dark Cubed and has extensive analytical and research experience in cyber security. He joined Dark Cubed from ZeroFox where he served as an open source intelligence and social media analyst supporting Fortune 500 customers.

dark3