Determining security assurance levels for your IoT products

Empowering Trust®

Executive summary

Not so long ago, little of our information and systems were digitized. If we go back to just 1989, the World Wide Web was only just being invented, and no home users had any real access to the internet at large. Our pictures were still being taken on film, and digital photography wouldn't be brought into the mainstream until 1994 when Apple released the first digital camera and 2000 when the Canon Ixus appeared on the market. During the early '90s, most people didn't have mobile phones, and those who did carried them in suitcases due to their size.

Malicious software at that time, such as it was, consisted mainly of academic research projects and nuisance programs that were written for fun. Such a program could not encrypt our family pictures and ask for money to have them returned, it could not capture recordings of us in our own homes for blackmail, it could not take control of our heating or front door locks and it could not recruit the devices we had brought into our homes to be used as part of a global army capable of bringing internet traffic around the world to its knees.

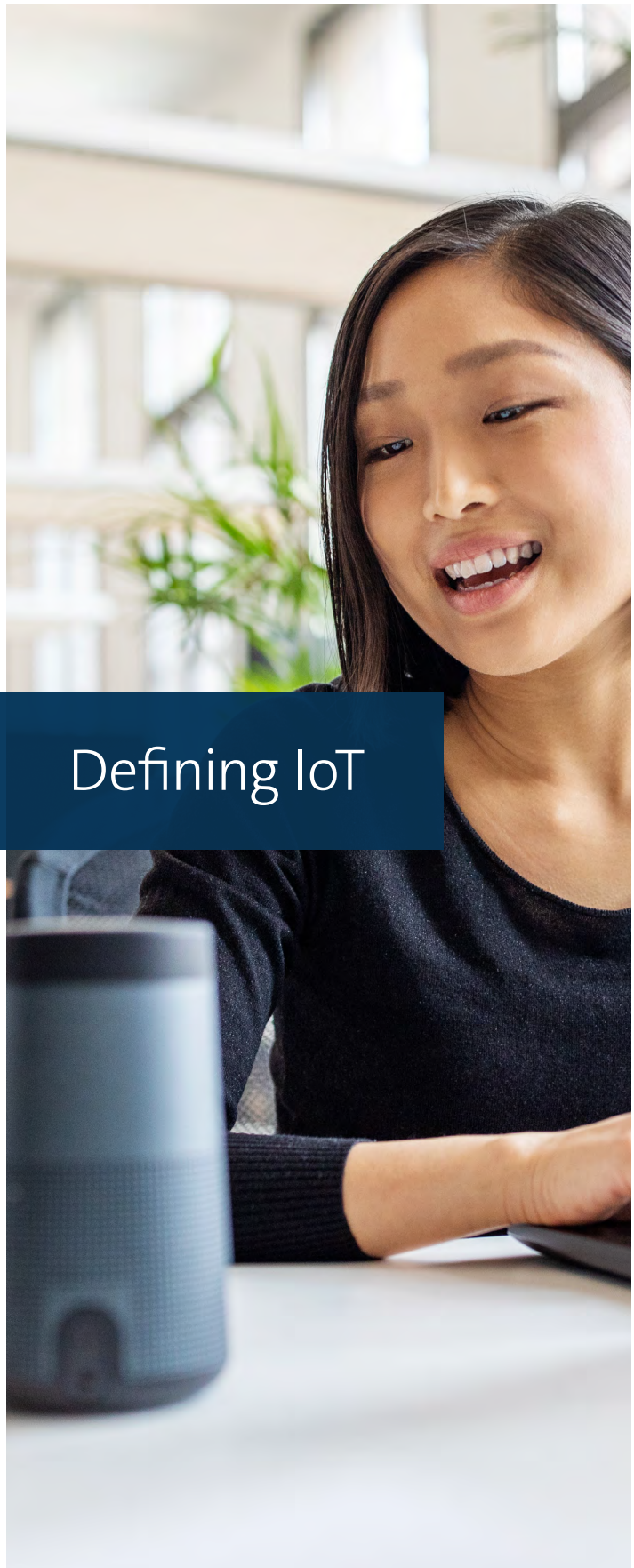
It could not do these things because most of our data and systems were still very much analog. In 1989, safety and security were essentially synonymous words that both effectively meant physical security.

Today — merely 30 years later — we have entrusted control of our data and sometimes our very lives to the computing systems around us. Physical safety, and the security of our data, money and assets, must always consider the security of the software in the systems that control or have access to these things.

And *everything* has software in it these days.

This has been understood in the context of general purpose computer systems for some time now, certainly since the mid-1990s when use of the internet dramatically increased with the world wide web. However, we are now facing a new stage of evolution for our connected systems — that of the IoT — bringing with it new concerns and requirements for security.

This document will discuss the definition of IoT and why IoT security is a more difficult problem to address than the security of general purpose computing devices. Moreover the whitepaper will dive into how IoT security can be best addressed by understanding the risks involved and using ratings of the security implemented in IoT systems to inform purchase decisions, and determining which rating is right for your product.



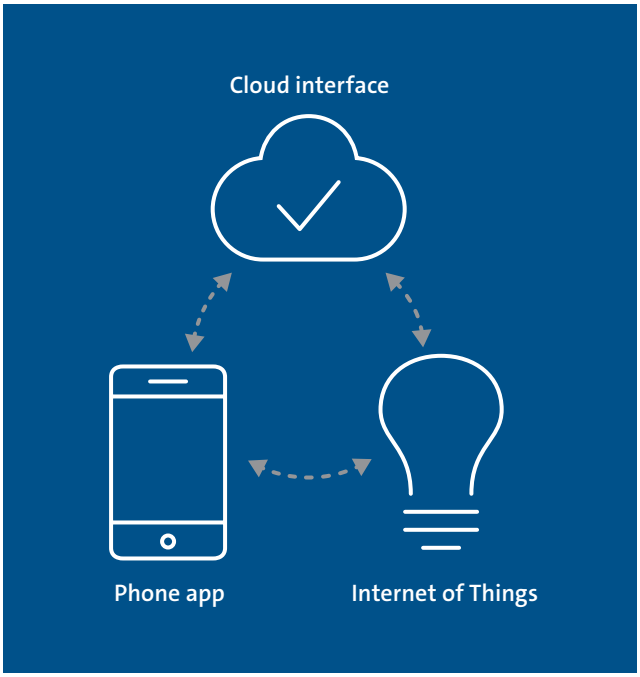
Defining IoT

Although the term IoT literally stands for “Internet of Things,” it’s harder to clearly define what does and does not fall into the definition of IoT. Many smart devices do not directly connect to the internet — using proxies such as hubs or using only local connections over Bluetooth or Zigbee wireless. The vast majority of IoT systems have companion apps or cloud services that either augment or are effectively essential for the operation of the “thing” itself.

For the purposes of this document, we will use the term IoT to refer to any collection of functions that includes at least one physical component that can be connected to over a switched or wireless network. The scope then includes all components of that system: the physical components, the resident software inside its various computing elements and any software residing in a mobile app or cloud instance.

This way, we include in the definition things like Bluetooth speakers and door locks that may not normally have connections to the internet at all. This is an important definition, as the security of a door lock is clearly a matter of importance, while that of a speaker is perhaps considered less so.

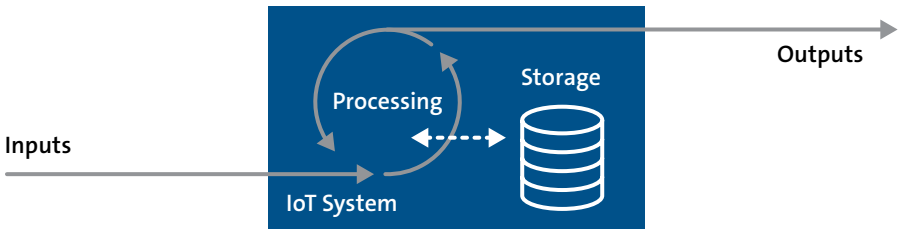
Why would we consider the security of these two things differently when they connect using the same wireless technology? What rules can we use to determine the threats that apply to any type of device, and what do those threats imply about the security levels required of that device?



The Risks of IoT

When assessing the security required for any IoT system, it's important to understand the risks that are faced by that system, what can go wrong and why a malicious party would be interested in compromising that system. Essentially this comes down to opportunity and value: how easily can a system be accessed and how much value can a malicious party gain from such access and/or compromise (essentially what is the target asset of the attack).

At the most fundamental level, any computing system — including IoT — can be summarized as a system of inputs, outputs, storage and processing, as illustrated below:



Most of the time, the focus is on the inputs, the user data, as the defining factor for why an IoT system may be attacked. However all aspects — the storage, processing power, output bandwidth and data, network functions, and location of a device — may be considered assets inherently valuable to an attacker. For example, a camera that points away from your house may be considered to have low value data. But that same camera could be compromised to become part of a botnet of never-before-seen scale, used by criminals to see when you leave the house or hide their approach, compromise the privacy of others in your street or attacked as the first stage of a multiple attack on the wider network.

Examples of assets an IoT system can have that may be targeted by an attacker, how these may be targeted and for what purposes is summarized in the table below:

Target Asset	Type of Attack	Example Goal/Purpose of Attack
Data stored or accessed	Theft of data	Monetization/blackmail
	Modification of data	Ransomware
	Extraction of system-wide data or code	Reverse engineering of code
Processing power	Use of processing resources	Cryptocurrency mining Password cracking
System operation/functions	Disabling of operation	Ransomware/blackmail
	Alteration of operation	Looping security camera footage
	Determination of operation	Determine if people are at home
	Exploitation of privileged operations	Open locked door
Network operation/functions	Use of bandwidth	DDoS attack
	Exploitation of trusted network functions	DNS modification
Network location	Access to other networks or systems	To attack other systems
	Capture of network traffic	Steal data from other systems

Because of this plurality of threats, it's unfortunately not easy to say if any particular type of IoT device or system has any value to an attacker. That value is often determined by the way the system is deployed and used, rather than the type of system it is.

Put another way, the security of IoT systems is more about where it is located and the data and resources the system has access to rather than what it is. The "what" may help define the data and resources, but it's not the primary factor. A smart speaker that's connected directly to the internet and provides internal views of the house through an integrated camera with large processing and bandwidth resources is a more attractive target than a Bluetooth speaker that simply plays music from a connected phone.

The IoT Security Problem

Understanding these many aspects to IoT security — the types of threats and risks involved — it's clear that there is a need to address security in these systems. However, that's not always a simple thing either. IoT systems are often a collection of different processing elements and different code that's executed in different locations with different physical and logical security. If the "where" is important, having multiple "where's" can only make things more complex.

And complexity is the enemy of security.

A fundamental problem with IoT security is that, although security often does not have to cost a lot of money to implement well, it does not come for free. Good security is a function of good design, which implies more time and knowledge in the initial phases of the product development. The more complex the design, the more elements and types of code involved, the more difficult it is to integrate the whole into a secure system.

Maintaining complex systems is equally fraught. Keeping systems up to date over time with patches and security updates requires having personnel to do it: personnel who understand what security means for the products they are creating today, and are able to keep up with updates in security research to know what security will be tomorrow as well, but who are working on products after the initial revenue for that product has been claimed. The more complex a system, the harder it is to keep up with all of the security issues, and the more people required to do it.

Given the global demands for their skills, these people often come at a premium. Therefore, good design and on-going maintenance has a tangible cost, as functions of the additional labor and time required. Equally importantly, the actual testing and validation of security features comes at a cost as well. "Quick" security testing can possibly be performed for lower cost, but that gives only a low level of assurance to the security property that is being tested. To gain more assurance, you need to perform more detailed testing, which takes more time and costs more money. That cost adds onto the cost of design and maintenance, which in total must either eat into the already thin margins of the IoT systems or increase their price at the point of purchase.

Because of this, at its root, security is in fact primarily a *commercial* problem.

Rating IoT Security

How do we accommodate for this cost of security? If we consider that security cost can only be some maximum percentage of the overall cost of a device (otherwise consumers will look to other solutions to buy), it then must be considered that lower cost devices may need to manage with lesser levels of security. This is not to say that there should not be an acceptable base level of security for any and all devices, but that the determination of the acceptable level may be a function of the device type and implementation.

However, security cannot be purely driven by cost either. We've already demonstrated that the likelihood of attack of a system is more about where than what. Fortunately often (although *unfortunately* not always), a correlation exists between the accessibility of a system and it's cost to the consumer. For example, IoT lightbulbs often connect over short-distance wireless such as Zigbee, and are therefore not directly accessible over the internet. Therefore, the risk posed by these systems is reduced: they cannot access the user's LAN directly, are not directly accessible by attackers over the internet, contain no sensitive data and have very little processing or bandwidth resources.

An attacker may be able to use a lightbulb to help determine if a person is at home, so security is still important for these products, but these devices are often accessed or grouped through a hub, which provides additional security features. Finally, all of this is then connected behind a router or firewall which (hopefully) provides even more security defenses to the internal network.

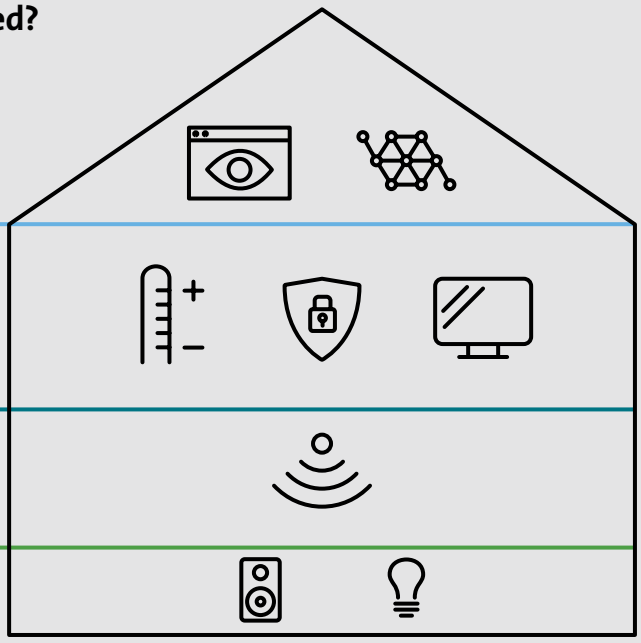
So lightbulbs may not need a high level of security assurance, but the hubs they connect to probably do. Routers and firewalls need the highest levels of security, as do other devices which may allow for direct access to the internet through the firewall despite any other security features of the network.

This gives us a layered view of the security required for systems in a home, office, or other environment, with the layers defined by accessibility and value of the system itself. This type of layering is illustrated below.

Systems that are less accessible, and have less valuable resources and data, can essentially meet a lower level of security — a lower level of security assurance — than those

How much security assurance does a device need?

	Example products	
High assurance Devices directly accessible from the internet Internet perimeter or security devices	• Cameras • Baby or pet monitors • Routers, modems • Internet exposed hubs	
High-to-medium assurance Devices with "smart" safety-related functions which may or may not be directly internet-connected Devices with access to the internet	• Heaters • Door locks • TVs • Voice-controlled speakers	
Medium-to-low assurance Devices bridging networks to LAN but not directly to the internet	• Local hubs • Bridges • Access points	
Low assurance Devices not directly connected to the LAN	• Bluetooth speakers • Lightbulbs (non-wifi)	



devices on the periphery of the network, which need a higher rating. Of course, these acceptable levels of security are in large part dependent on how the IoT systems are deployed and used, which is often difficult to determine by a manufacturer prior to sale. A customer may in fact decide to use Wi-Fi lightbulbs and connect them directly to the internet, which will increase the risk and therefore require increased levels of security.

However, there are some general questions that may be asked to help determine the risks posed by a system, and therefore the security level that is required. These are provided in the table to the right, showing recommendations for high levels of assurance to lower levels of assurance. The top item that is true for any system is the intended level. For example, consider a Bluetooth door lock. It may only be accessible over non-internet routable connections (which is recommended for a low level of assurance), but as it provides physical safety and security related functions, a high level of security assurance is instead appropriate.

Using this table, manufacturers and vendors are able to easily determine what minimum level of assurance is appropriate for their products. This does not mean that higher levels are not a good idea. Higher is always better, and can help with differentiation of products in the market. This table is provided only as an initial guideline to help determine a minimum level that may be suitable.

It's also expected that these recommendations may change over time, or the requirements and assurance at each level may change, as the overall security maturity of the IoT landscape improves. This would be similar to how the Australasian New Car Assessment Program (ANCAP) car safety standard has included additional safety items over time, as car safety has improved.

Now that we have a guideline for what levels may be appropriate, we also need a way to illustrate to the purchaser of the IoT system what level of security an IoT system has actually achieved, how it has been assessed and what it implies for the expected deployment of the system. This allows the user to select a system that may be more costly, but with a higher security rating, if they are intending to deploy it in a way that implies more risk, such as connecting it to the internet, using it for sensitive data storage or processing, or connecting it to other high-value systems.

Increasing baseline security, and enabling customers to choose security options that suit their needs, is the role of security rating systems.

System Scoping Question	Minimum Recommended Security Assurance Level
Does the system implement safety or security related functions, such as HVAC control, network or physical security?	High
Does the system require, or can be configured to have, a direct connection from the internet?	High
Does the system have access to sensitive data, such as video or audio recordings, payment details, etc.?	Medium to High
Does the system (even if a hub that connects other systems) allow for direct connection to the internet (connect out, rather than connect in as above)?	Medium to High
Does the system act as a hub or bridge between different networks to the customer LAN, but does not directly provide internet access?	Medium to Low
Is the system only accessible over low bandwidth, non-internet routable networks such as Zigbee, or Bluetooth audio?	Low

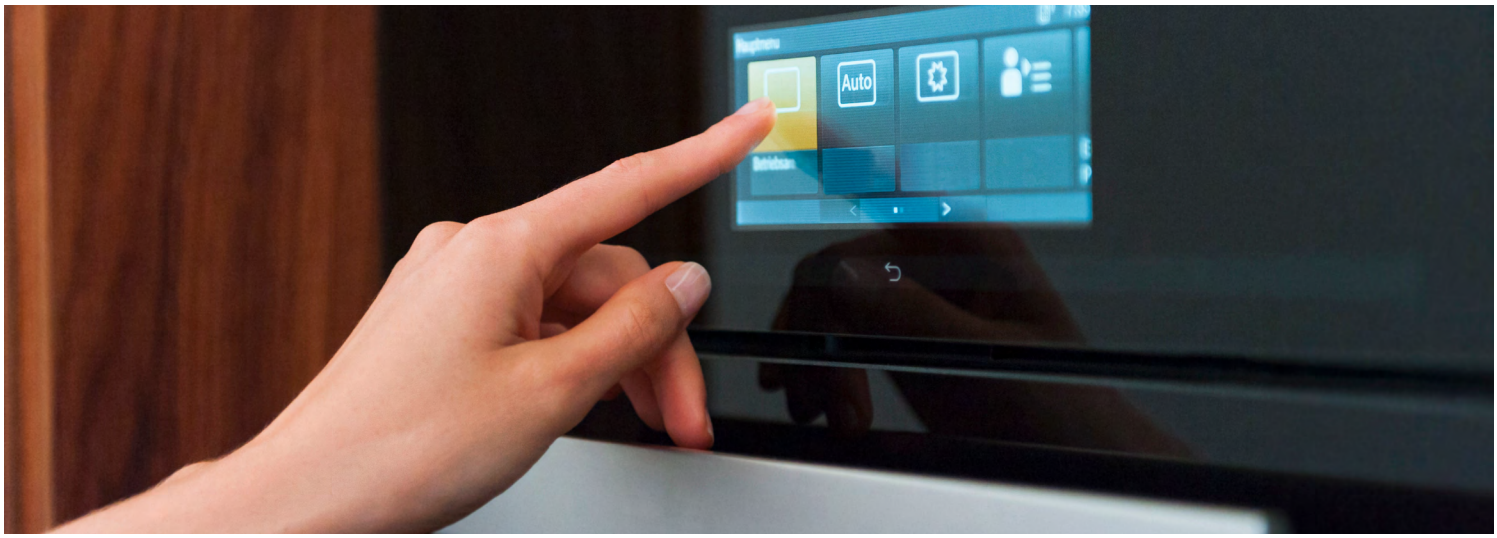
The Security Journey

Another value of rating the security of systems, rather than providing a binary secure/insecure output, is that it helps incentivize investment and growth in IoT security. It's unrealistic to expect that all products released tomorrow are going to automatically meet the highest standards that can be set for security. Indeed, it's likely that meeting these highest levels will only be possible with a complete redesign, or very large cultural changes in the way in which products are designed, built, shipped and maintained.

This presents a quandary for a pass/fail security program. Do we drop the level of the requirements to the minimum level that is achievable by most products today, understanding that this is not the end level we actually want to achieve, or do we set the bar to where we believe it should be and simply wait for the industry to catch up?

If the bar is set too low, we can at least have some validation of minimum requirements, but there would be no incentive or recognition for companies to exceed these requirements to demonstrate their concern for their customers. If the bar is set too high, we can be sure that products that meet these requirements are very secure, but it does no good if nothing can meet the level and the entire industry is disincentivized.

Either way fails to provide useful information to consumers about how different products have applied and implemented their security practices.



Addressing IoT Security Through Ratings – A Commercial Solution

Driving an increased level of security maturity in IoT systems requires an understanding of both the commercial aspects that drive IoT design and deployment, as well as the risks that inform the level of assurance that is required for different product types and uses. That risk is a function of many different factors: what data the system can access, how much bandwidth and processing power it has, what other systems it has access to or control over and how easily that IoT system can be accessed and compromised.

Ideally, IoT security could be addressed objectively as a binary secure/not secure, but this is just not possible and does not provide a fair representation of the efforts taken by the industry. Achieving the highest levels of security does not occur by accident, and both secure product design and security testing takes time and costs money. This impacts the commercial viability of products, potentially reducing the ability to spend money on securing the next generation of devices.

With legislation coming that mandates certain minimums for IoT security, and various industry bodies working on their own sets of IoT security requirements, what are the best ways to achieve compliance, compete in the market, and still maintain a commercially viable product range?

To answer this question, we cannot expect the highest levels of security for all systems from the outset. This is just not a commercially feasible stance. Instead, we need to adopt a staged approach to IoT security and drive a minimum base of security for all devices, with increasing security for systems posing greater risk.

Over time, as the market understanding for both the need and design of security grows, the levels and systems to which these are applied can be increased. This awareness will help increase the commercial pressure for secure systems. At the moment, customers have either given up on IoT security altogether or simply expect security to be baked in without any real understanding of whether it is or not. To solve this issue, we need to make security more visible to the consumer. But without levels, we are left with either accepting the lowest levels that can be commonly achieved or preventing the adoption of security standards that require too rapid a change in security posture.

Improving security must involve working with the industry rather than against it. We must provide solutions rather than simply cataloging the issues and ensure that the commercial aspects of security are addressed. To do this, we must be able to easily demonstrate to consumers which products have spent more time and effort on their security posture, and that can only be achieved through a rating methodology.

Which rating is the right one for you, or your products? To answer that, you need to understand your market, your customers and the way in which your technology is used. The layered approach presented in this document, using information about access and assets, provides a quick way to make that determination.

To learn more, contact UL at IMSecurity@ul.com or visit IMS.UL.com/IoT-Security-Rating.

UL Cybersecurity

UL's IoT Security Rating joins a growing list of UL IoT security solutions, including the UL Supplier Cyber Trust Level, UL Cybersecurity Assurance Program, IEC 62443 and other training and advisory services, that address security assessments across ecosystems, supply chain safety and quality, and markets regulated for security.

About UL

UL helps create a better world by applying science to solve safety, security and sustainability challenges. We empower trust by enabling the safe adoption of innovative new products and technologies. Everyone at UL shares a passion to make the world a safer place. All of our work, from independent research and standards development, to testing and certification, to providing analytical and digital solutions, helps improve global well-being. Businesses, industries, governments, regulatory authorities and the public put their trust in us so they can make smarter decisions.

To learn more, visit UL.com.

UL.com

0220