ioXt
internet of secure things

The ioXt Security Pledge

8 PRINCIPLES FOR CONSUMER PRODUCT DESIGN AND MANUFACTURING TO ENSURE SECURITY, UPGRADABILITY & TRANSPARENCY

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We're living in exciting, fast-paced times. Some would even call it the future. With all our digital devices, chosen and unchosen, connected to the internet, we have convenience, speed and flexibility in our daily lives like never before.

And it just keeps evolving.

But with this constant innovation, we also face genuine risks and threats from those who want to walk through any virtual door that's part of our digital footprint. The exponential growth of the Internet of Things (IoT) compounds threats to our security and privacy.

With all that increased connectivity—and new internet-connected home devices—on the horizon come legitimate questions and concerns about security. How do we tackle it in a way that's expedient and beneficial to everyone, to provide what consumers need and to guide manufacturers and service providers with best design practices so that the result is a more stable and secure national, if not global, landscape?

The answer is the **ioXt Security Pledge.**

The ioXt Security Pledge is the result of industry working together to set security standards that bring **security, upgradability** and **transparency** to the market and directly into the hands of consumers.

INTRODUCTION

For many people, there's a real air of anticipation around talk of the Internet of Things. IoT, as it's called, means devices from many different networks will be connected in new and often unexpected ways to solve real world problems and transform daily life.

Motion sensors in a home, for example, could control lighting, the HVAC and security systems—even sleep mode for the office printer. With all this connectedness, security will need to be defined at the product level, not the low-level protocol layer. And upgradability of devices and transparency with the consumer will be just as important as security.

The way to do that is to start at the beginning, by building security into IoT products. By identifying and clearly defining best practices, supporting the implementation of those best practices and establishing consistency in consumer labeling of products and services, we can help create consistency and compliance across industries and protect consumers.

And, while we may not eliminate insecure consumer IoT devices—those with systemic security issues that leak consumer data—from the marketplace, we can provide an easy way for retailers and consumers to know which IoT products are safe and secure.

The ioXt Security Pledge is the foundation for making this happen. It will remove any guesswork from creating secure, well-designed products, as well as establish a way for identifying all products and services that comply with ioXt Pledge standards.

By ensuring device security, upgradability and transparency, the Pledge assures retailers they're offering safe products and assures consumers they're making an intelligent (not just a "smart") buy.

The ioXt Security Pledge is composed of eight clear principles:

1. The product shall not have a universal password; unique security credentials will be required for operation.
2. All product interfaces shall be appropriately secured by the manufacturer.
3. Product security shall use strong, proven, updatable cryptography using open, peer-reviewed methods and algorithms.
4. Product security shall be appropriately enabled by default by the manufacturer.
5. The product shall only support signed software updates.
6. The manufacturer shall act quickly to apply timely security updates.
7. The manufacturer shall implement a vulnerability reporting program, which will be addressed in a timely manner.
8. The manufacturer shall be transparent about the period of time that security updates will be provided.

The rest of this booklet further describes each of the Pledge principles and how they are included in the design and manufacturing of consumer products.

1. No universal passwords

The product shall not have a universal password; unique security credentials will be required for operation. Universal passwords allow an attacker to easily gain access to any device. Therefore, products shall either have a unique password or require the user to enter a new password immediately upon first use.

Universal passwords are one of the security vulnerabilities of connected devices. Too few consumers ever change the default password of a device, and it has become easy for attackers to share known password lists and gain access to consumers' homes.

Ideally, every device should have a unique factory-programmed password. This password could be shared with the user through a sticker or QR code on the device. For instances where it's not desirable for a sticker to be visible or accessible, the product can require a new password to be entered immediately during device installation. Ideally, this password will be significantly difficult to "crack."

The primary goal for disallowing universal passwords is to prevent remote attackers from guessing a product's password—let alone gaining control of every unit for a given device model.

In other words, this principle makes it virtually impossible for a fresh out-of-the box device to be hacked remotely by requiring each new device to either come with its own unique password or require the user to create a password before the device can operate.

2. Secured interfaces

All product interfaces shall be appropriately secured by the manufacturer.

The nature of connected products is that they can communicate with each other to realize product experiences in the home. Think, for example, about how your smart light bulbs communicate with your remote. Because of this interconnectivity, all sensitive interfaces which could be remotely accessed and attacked should be secured against breach, modification and monitoring.

Therefore, all product interfaces shall be appropriately secured. Not all devices are created or used equally; therefore, not all devices have the same attack surface. At a minimum, all devices shall be secured from remote attack. In addition, some devices may also be protected against local attack.

For example, a connected light bulb needs to be protected against remote attack. But it's unlikely a homeowner will be motivated to remove the glass and inject malicious code into their network—barring any need for local protection. Cable set-top boxes, on the other hand, need to be protected against remote as well as local attack.

In all cases, any external communication interfaces shall be secured.

For products in which local attacks are a concern, internal chip-to-chip interfaces may be secured. Further, memory interface may also be secured through secure boot or other memory integrity checks.

All sensitive interfaces shall be encrypted and authenticated.

This principle requires consumer product manufacturers to implement "secure by design" measures that will best protect a device against product interfaces, given device type and intended usage.

3. Proven cryptography

Product security shall use strong, proven, updatable cryptography using open, peer-reviewed methods and algorithms.

Industry needs freedom—and the strength of community—to constantly improve. A perfect example of this is cryptography, where allowing all professionals to come together leads to the best possible security solutions.

ioXt Security Pledge participants agree their product's security shall use proven and standardized cryptography. Specifically, suitable cryptographic security techniques and algorithms that are well developed, proven, reviewed and standardized and should be applied wherever possible in place of proprietary developed algorithms, which haven't been subjected to the same level of scrutiny and review.

Open standards, in addition to increasing interoperability and consumer choice, are inherently more secure than proprietary implementations. In open standards organizations and in practice, many more companies, engineers and other stakeholders not only bring their expertise, best practices and work to the technology, but continuously evaluate security practices and testing against vulnerabilities. This allows open standards to be designed with security in mind and to evolve quickly; they're resilient against new security threats.

When it comes to problem-solving, there are those who work alone and those who collaborate, using the power of community to achieve optimum results. Because open standards often provide the nimblest way to address security vulnerabilities, this principle requires companies to start with well-known and current encryption methods and finish by making sure new security methods are peer reviewed.

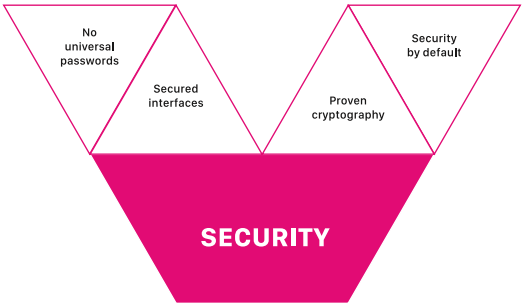
4. Security by default

Product security shall be appropriately enabled by default by the manufacturer.

As a user, you have a reasonable expectation that a new product comes with an appropriate amount of security protection. You can turn off that protection if you want—say, to digitally venture outside the App Store, where apps are audited and secured, and choose to download a third-party, possibly unsecured app. But nothing should be required of you to begin with to make the device secure. It should be enabled by default by the device manufacturer.

Just as you can choose to have lower-than-default levels of security, you can also enable higher levels of security—such as disallowing your child to make in-app purchases through their phone. Again, what's important is that there's an expected level of security, a baseline that comes automatically with the device.

This principle guarantees that products are appropriately secured at the time of purchase. While the consumer can choose to step up or step down this security level, the manufacturer will not leave the consumer unprotected by default.



5. Signed software updates

The product shall only support signed software updates. While it is critical that all products be updatable, it is just as critical that these update images be secured. A manufacturer must cryptographically sign update images to prevent tampering during deployment. The product must not use unsigned updates, as they could be fraudulent.

As hard as companies try to avoid them, software bugs are bound to occur. Plus, security is always a rising bar. An action considered acceptable a few years ago—such as a simple CRC to protect an image from accidental corruption—may be used as a simple attack. Thus, a product must have a way to deploy new updates.

However, injecting new code into a device presents a security threat in itself, as attackers could use this path to repurpose a device into a bot. Therefore, the update images released by the manufacturer must be cryptographically signed. Further, the product must validate all update images prior to using the image.

It should be noted the requirement for signed software updates doesn't necessarily require secure boot, which would verify the current image every time the device powers up. Signed software updates provide protection against remote attackers, which is a common requirement for all connected devices. Secure boot prevents against local attacks, where the attacker has possession of the product.

This principle ensures only properly identified software updates will be accepted by a device.

6. Automatically applied updates

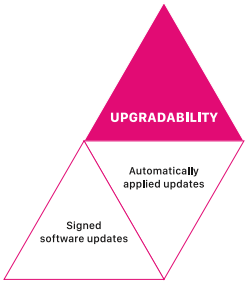
The manufacturer will act quickly to apply timely security updates. Whenever a security vulnerability is detected, the manufacturer will automatically apply a patch to the product. No user intervention will be required.

Does your security camera need updating? That's a question a consumer should never have to ponder. In other words, a user shouldn't have to be the administrator for their devices. And they certainly shouldn't have to be a security expert to ensure any updates are applied properly and quickly.

In fact, addressing any updates or critical security defects shouldn't require user interaction. Thus, the manufacturer will automatically deploy security patches in a timely manner. Not all products can be deployed immediately, in which case an update may be slightly deferred.

For example, a connected car's braking system may be updated once the car is parked—to do so sooner could compromise driver safety. Or, since many connected devices are deployed over large geographic areas, a manufacturer could choose to deploy a security update region by region, to reduce the peak data traffic through their networks. In other cases, some products may be moving through the supply chain, and be updated once connected for the first time to the network.

This principle ensures that when consumers buy a connected product, the device will be automatically secured and updated throughout its lifetime and that security updates will be applied as soon as is reasonably possible.



7. Vulnerability reporting program

The manufacturer shall implement a vulnerability reporting program, which will be addressed in a timely manner. All companies that offer internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.

As a consumer—or even a researcher—when there's something wrong with a device or its service, who you gonna call? Whom should you contact and how can you be sure they received your feedback, so they can do something about it?

The device manufacturer or service provider shall operate a vulnerability disclosure program that allows users, organizations and researchers to communicate their concerns about security issues and even share developments around new security techniques. Such a program will be put into place to allow newly identified vulnerabilities to be responsibly disclosed and to be addressed quickly, if necessary.

This principle provides a means for companies to listen to their customers and to developers in the industry. Having a vulnerability reporting program builds customer care around security by creating a path for direct communication and accountability.

8. Security expiration date

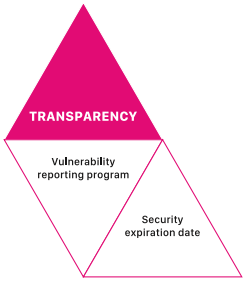
The manufacturer shall be transparent about the period of time that security updates will be provided. Like a manufacturer's product warranty, there shall be transparency around the support period of security updates.

When you buy a product, say a TV, microwave or laptop, you know the manufacturer's warranty is usually one year. Typically, the product comes with a registration card that highlights this fact. As a consumer, you should know what you're getting warranty-wise with your purchase; security updates are no different.

Consumers should be aware of the length of time a manufacturer will support product security. While a manufacturer is not expected to support a device forever, a consumer should be able to make an informed decision around the expected security lifetime of any product they purchase.

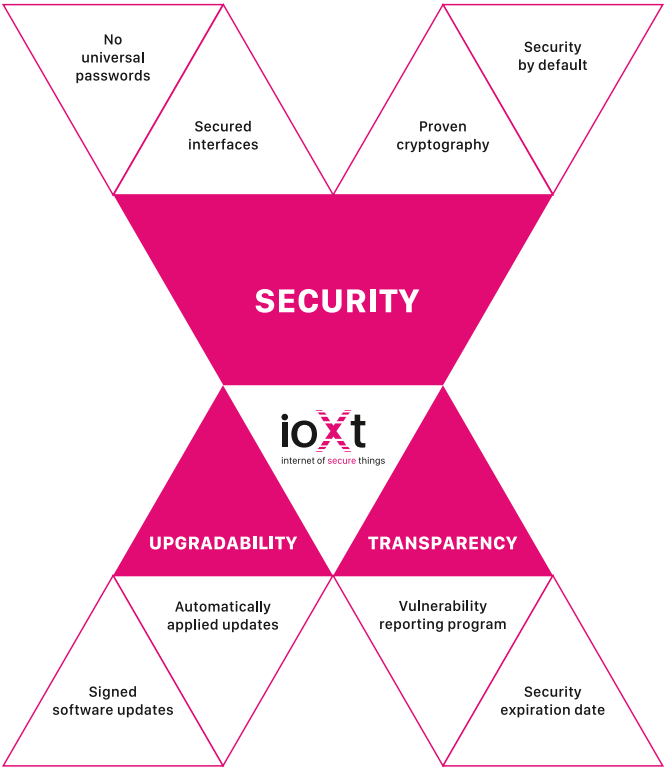
The manufacturer's security coverage period will be clearly communicated. Some manufacturers may offer extended security warranties to help offset the continued engineering cost, while other companies may offer products with a reduced warranty at lower product cost. Whichever model a manufacturer chooses, the consumer will be given the information to make an informed purchasing decision.

This principle assures consumers there will be no guesswork about the duration of security updates. Therefore, there will be transparency about how long your device receives security support.



The ioXt Security Pledge was created collaboratively by leading consumer products companies, standards groups, compliance labs and government organizations.

With eight principles built around the goals of providing security, upgradability and transparency, the Pledge helps define IoT product security excellence and steer all related industry towards a new highly-connected, yet secure, frontier.



For the latest information on the ioXt Security Pledge and how to participate, or for a list of companies whose products or services comply with the Pledge, visit ioXtAlliance.org.