Challenges and Practical Approaches to Consumer Software Labeling

ioXt is an Alliance of leading technology manufacturers, service and platform providers, silicon manufacturers, and retailers working together to increase the confidence of consumers around the security of connected products and services. The Alliance has over 500 member companies supporting Smart Home, Smart Building, Cellular, and mobile application markets. It is our goal to promote a set of harmonized security standards which are testable, scalable, and impactful to the end consumer. We have certified over 120 devices ranging from connected dog collars to smartphones, building controllers to mobile applications such as VPNs. We provide security transparency to the end consumer through our certification mark and live label which allows consumers to see the latest security stance of any certified product prior to purchase.

How different conformity assessment (vendor attestation, third party assessment) approaches can be employed in consumer software labeling efforts?

The biggest challenge for any conformance program is balancing the vendor's compliance to the security standard while not adding too much burden (i.e. time or cost) to the already complex development schedules required to launch products on a global scale. Vendor attestation programs offer lower cost and significantly reduced times as compared to existing US programs (such as FIPS). Vendors may be tempted to abuse these programs. However, they do carry potential legal damages for posting false information. More often than not, the vendors may make honest mistakes as they may not be familiar with the intricate requirements of many security compliance programs. This may put consumers at risk and may not be appropriate for all types of products.

The ioXt Alliance strengthens our vendor attestation program through the use of a researcher reward program. Essentially, we provide a publicly available portal in which anyone can view the vendor's compliance record and then we reward researchers who can disprove any of the compliance data. The Alliance works with the researcher to validate the submission and then engages the vendor to correct the issue. If the issue is determined to be valid and the vendor does not make a correction to their compliance record then the product is removed from the compliant product list and the live label is retracted. It should be noted that financial rewards are helpful, but not critical as many researchers and universities are engaged in security research for publication. Often a security issue ties back to a compliance issue. Also, stocking retailers have expressed concern at the cost to remove products which may no longer be compliant.

Third party assessments are also critical to any compliance program, as this method tends to produce higher levels of assurance to the end consumer while reducing liabilities for the vendor. We have found that some channels or products will only accept third party assessments as it provides a higher level of assurance immediately at product launch, as compared to the potential lag from the researcher rewards program.

There are many challenges in testing IoT product lines. Many companies produce thousands of different SKUs and combinations. Further, the breadth of IoT devices is large and thus difficult to build detailed explicit test cases for all aspects of the product's security. Oversight of the labs is critical, but a council which can provide technical direction is far more important. Further, the researcher rewards program is valuable in monitoring the performance of lab certifications and enabling continuous assessments of the product after launch.

The ioXt Alliance recommends the use of both vendor attestation and third party assessment. However, the vendor attestation must have some form of continuous validation and may not be appropriate for all markets or devices.

Feasibility and possible means for implementing tiered labels that reflect increasingly comprehensive levels of testing and assessment

All devices share a common baseline set of security requirements. However, this baseline may not include all the security requirements needed for all devices. Further, different devices will require different security controls. For example, a light bulb which has limited connectivity bandwidth, processor power, and memory may not need the same controls as a camera running linux with a high bandwidth WiFi link. One may be tempted to give the light bulb a bronze rating and the camera a gold rating. However, the consumer may interpret this to mean the light bulb is NOT secure and should be avoided.

Further, different devices may also require different controls. For example, commercial lighting systems have a higher set of requirements around resilience and reliability, while smart speakers may need more controls around privacy. The ioXt Alliance provides a set of profiles for different devices and markets. Devices must be certified against the required profiles and then receive a common compliance mark. Thus, when a consumer sees the compliance mark, they know that the device is secured for its use, but do not need to know all the intricacies of security testing and threat modeling.

The ioXt Alliance provides a compliance program with product labeling which supports the simple binary compliance mark with a live label which allows for further information regarding the security controls that have been implemented along with the assessment means used to validate the claims. The following is a high level description of our process.

1. The vendor selects the security profile based on the product or service they are certifying.

2. The profile describes the minimum set of security controls they must implement in their device and organization. The profile also contains optional controls which may be implemented by the product or service.
3. The vendor either performs the assessment themselves or engages an ioXt Alliance approved lab to perform the assessment.
4. Once all minimum security requirements are implemented and validated, the vendor's test results are published on the ioXt Alliance website, The vendor is issued the compliance mark and corresponding live label which points back to the product on the ioXt Alliance website.
5. When a customer looks at the product on a shelf, they can see the compliance mark which indicates that the product has met the security requirements for the product type they are buying. They can also scan the live label to see detailed information regarding the product.

We advocate a live label represented by a simple QR code. The live label is necessary because security is never static - an unpatched device may become unsafe at any time in the future. The label gives the user real-time information about the security status. The QR code is familiar and easy to understand - the QR code scan resolves to the current active security certification page for the product, which will include whether the security certification is still valid, the security expiration date, and other important baseline security information for the product. As described above, the ioXt Alliance is already using this simple live label.

Measures for incentivizing participation by consumer software developers

Conformance assessment for IoT will fail if every country establishes its own bespoke scheme. Manufacturers will be unable to manage and support such complexity. We need a conformance scheme that can be used globally with cross recognition between the schemes established up front, not done as an afterthought. The traditional approach of each country doing its own thing is the biggest risk to progress in raising the security bar in IoT. With the ioXt Alliance, we've created an international non-profit with international regulatory advisorship to protect against this. We are encouraged that NIST is helping to lead the way in labeling programs, and want to see alignment at the global level.

Product developers strive to create products negotiating competing requirements on security, privacy on one hand and time to market and competitive features on the other. Product teams can easily measure and assign return on investment for many aspects of a product. Security, safety, and privacy are less direct. For these aspects of a product, any mandates from the customer, channel, or regulatory body instantly prioritizes the required development and investment. Care needs to be taken to balance the mandatory requirements such that they protect the consumer, are scalable across the global market, and do not stifle innovation and competition.

Several incentives could be used to increase participation by the developers. The following is a short list of potential incentives.

- Limits on the penalties for security incidents for products which participate in the program.
- Require products which are purchased by federal and state governments to implement the label.
- Require products used to receive tax incentives to implement the label.
- Encourage energy efficiency programs to require products to implement the label.
- Motivate insurance companies to provide a discount to companies who are providing services based on connected products which implement the label, or consumers using said services.
- Cross recognized security certifications such that manufacturers do not need to retest in every region they are deploying products and services.

Conclusion

The ioXt Alliance has an active compliance and security labeling program for Smart Home, Smart Building, Cellular Devices, and Mobile Applications. We believe that manufacturers should be transparent around the security provided by their products or services. This allows consumers to make informed decisions. However, we warn against fragmentation as it creates undue burden and overhead for manufacturers. Further, consumer labeling must provide clear messaging to the consumer as to what is "**good**" versus what is "**great**" and what actions they should take. A product with a one star rating may be better than one with no rating. However, consumers will avoid the one star products if they are sitting next to a three star product. The labeling scheme must reflect that the product has the "right" level of security for that type of device agreed upon by industry experts which is why a security scheme based on industry agreed Security Profiles is crucial for the success of any security labeling program. Finally, the label must actually mean basic security controls are in place. The entire effort will fail if labeled products are repeatedly demonstrated to be vulnerable to large scale attacks.

ioXt