SYNOPSYS®

Considerations in the launch of consumer cyber security labeling

Synopsys welcomes the opportunity to contribute to the NIST efforts to increase transparency and support consumer cyber labeling. Synopsys provides system and device developers worldwide with a combination of semiconductor design tools, reusable IP, and software security tooling and services. As such, the Synopsys approach to cyber security labeling comes from the perspective of the entire system design and the challenges in end-to-end system security including software, hardware, and supporting services.

Consumer device labeling can bring many benefits; however, Synopsys would like to highlight a number of considerations based upon our experience helping to design and security systems for leading global enterprises:

- **The communication goals of the label itself –** the need for clarity and ease of use by consumers
- **Initial details and level of additional detail –** key information at first sight, and refer to external resources
- **Validity and lifecycle management of the label and underlying certification(s) –** consumer awareness of changes to underlying certification or state of device security is critical
- **Interaction with external services, system architecture, and other obligations –** the need to provide visibility into where data is processed or stored, and the security status of those external dependencies

Clarity on communication goals of the device and packaging label

Throughout industry dialog, as well as both commercial and national device labels piloted internationally[1] [2] [3], there have been several variations on what information a consumer label is conveying to the user or prospective user. It appears that there is consensus on two general attributes:

- That the device has been developed according to best security practices, in some cases with no additional validation of this claim (other than potentially a self-attestation), and in some cases, whether or not a third-party organization has assessed and attests to these claims being true
- Communicating the fact that the device contains security features, functions, and capabilities (including, for example, the ability to receive updates – perhaps for a stated period of time), and whether the user must take specific actions to enable or utilize these – for example, configuring a strong default password or specifically enabling encryption functions

In prior studies, particularly the Harris Interactive study commissioned by the UK Department of Culture Media and Sport (DCMS)[4], even some of the simplest variants were found to be confusing to consumers. In 13% of those surveyed, where a date was quoted as the lifetime to receive updates, some participants felt that this implied an 'expiration date' for the device itself. From this study, it is clear that extensive consideration must be given to the clarity and style in which information is communicated – particularly since some consumers may use this as a pre-sales evaluation criterion when selecting between a range of competing devices. Furthermore, any scheme based solely on self-attestation is likely to carry much less weight, and therefore it is important to distinguish between those security assertions which have been verified by a competent third party and those which have not.

Level of detail communicated in label and availability of associated resources

Following the topic of clarity, is the question of whether the label should attempt to communicate all key information via the label itself, or whether there should be a link or other reference provided which may be used to look up further information. It is suggested that it might be helpful to include more verbose and explanatory labeling information on the packaging where more space is available, versus what is physically placed on the device itself where space may be constrained – and how a user may correlate these at a later date when the packaging has been disposed.

---

[1] *TRAFICOM, the Transport and Communications Agency of Finland, Cyber security labeling infopack for companies* https://tietoturvamerkki.fi/files/cybersecurity-label-infopack-for-companies.pdf

[2] *CSA, Cyber Security Agency of Singapore, Cybersecurity Labeling Scheme (CLS).* https://www.csa.gov.sg/Programmes/cybersecurity-labelling/about-cls

[3] *Rapid evidence assessment on labeling schemes and implications for consumer IoT security, Johnson & Blythe, University College London 2018* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949614/Rapid_evidence_assessment_IoT_security_oct_2018_V2.pdf

[4] *Consumer Internet of Things Security Labelling – Survey Research findings, Harris Interactive on behalf of UK Department of Culture Media and Sport, 2021* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950429/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report_V2.pdf

For example, the device could include a simple logo indicating the security 'status' – but might also include a QR code which links to a complete security analysis, additional configuration guidance, and a software bill of materials.

Synopsys suggests this hybrid approach – concise information readily available, but with a clear reference to supplementary information which a consumer may consult, such as post-purchase usage and configuration guidance – would provide the right balance of fast information to consumers yet still facilitate the dynamic nature of security evaluations which may be further updated during the device lifecycle.

Validity and lifecycle management of the label and supporting information

The security status of a given device may not be constant for many reasons (continual changes to the threat landscape, new vulnerability information, and potentially changes or updates to device software), and this means that the device labeling regime should take this into consideration. Any assessment (whether self-assessment or third party), therefore should be considered a 'point in time' analysis, and so the lifecycle design of the labeling system must accommodate this.

One key aspect of this is that of what action should be taken when the device software changes, whether a significant feature change may invalidate existing security label attestation, and in these circumstances whether any security assessment should be repeated. In other spheres, most notably the recent United Nations Economic Commission for Europe World Forum for Harmonization of Vehicle Regulations (UN ECE WP.29)[5], consideration is given to the scope and impact of the software change as a means of evaluating whether the functionality has deviated sufficiently to invalidate vehicle type approvals. It is suggested that a similar method could be employed for determining whether consumer device software attestation must be updated, or whether a label can be re-used following a small bug-fix update with no additional features.

Given the notion that the label itself contains only core information and that additional dynamic information would reside elsewhere and may require to be refreshed as new information occurs, this would imply that a consumer may need to periodically re-assess the security status of the devices in their homes. Once a large number of devices exist, and perhaps in inaccessible locations, this quickly becomes impractical. Therefore, consideration should be given to a machine-readable method by which this information could be transferred and re-assessed. The authors suggest protocols such as the recent IETF RFC for the Manufacturer Usage Descriptions (MUD) protocol[6], and its extensions[7], as a potential way in which this could be transferred to a central home hub or hosted external service as a means that consumers may evaluate compliance and become alerted to devices which require remedial actions.

Interaction and dependency on external services, and other obligations

It is commonly seen today that some consumer devices are almost entirely dependent on an external service hosted in the cloud. This poses the question of whether or not a device label should explain to a consumer what level of processing is carried out locally versus in an external cloud service, and what level of assurance that cloud service has, must also be considered. This may be security relevant for some consumers – knowing whether data is processed in a cloud service, and potentially a cloud service hosted outside of US borders, might be a concern – particularly for those living or working in high security environments such as military bases, smaller contractors who choose consumer rather than enterprise products, as well as those now working from home on confidential projects. The security of the surrounding home or office network must also be considered, and if the security of the device usage is dependent upon this, then the consumer should be made aware of best practices to assure the expected environmental configuration which the device would operate within.

Furthermore, some consumers may wish to understand the level of access for the purposes of repairability of their devices in line with emerging right-to-repair regulations – where the interaction between these and security goals must also be considered, particularly given that some security best practices may make the implementation of consumer access to the underlying device software and configuration more challenging (e.g. disabling debug access, encrypting and protecting firmware in transit at rest). Therefore, a security-compatible method for consumers to enable advanced access should be considered an essential design feature and labeling must not penalize device manufacturers for this.

---

[5] *UN regulation 156, Uniform Provisions concerning the approval with regards to software update and software update management system, January 2021.* https://unece.org/sites/default/files/2021-03/R156e.pdf

[6] *Manufacturer Usage Descriptions, Internet Engineering Task Force (IETF) Request for Comments (RFC) 8520* https://datatracker.ietf.org/doc/html/rfc8520

[7] *Discovering and Retrieving Software Transparency and Vulnerability Information, Internet Engineering Task Force (IETF) Draft reference draft-ietf-opsawg-sbom-access-02*. https://datatracker.ietf.org/doc/html/draft-ietf-opsawg-sbom-access