Red Alert Labs submission on consumer software labeling

Red Alert Labs wishes to thank NIST for extending to interested organizations like ours the opportunity to contribute our ideas on the challenges and practical approaches to consumer software labeling.

Red Alert Labs is a cybersecurity company specialized in consumer and IoT software. We have the rare combination of both technical and governance expertise required to assist governments and large stakeholders (Standards Development Organizations and large enterprises) in defining and operating ICT Cybersecurity certification schemes covering Certification Authorities and Evaluation Labs activities.

This paper focuses on the overall structure of a consumer software labeling program. Our recommendations are based on the experience from two current government programs, one European and one American. Note that these lessons could also be applied to the IoT device labeling program.

One characteristic of consumer software is its huge diversity. “Consumer software” can mean the software in a baby monitor, communications software, or a home banking application. The purpose of a consumer software labeling program is to educate consumers on the cybersecurity vulnerabilities that might be found in the software they use, as well as to certify whether the software developer has taken sufficient basic measures to mitigate the threats that could exploit such vulnerabilities, based on specific government-developed criteria. These threats fall into two broad categories: common threats that apply to almost all consumer software and specific threats that apply to some subset of consumer software.

An effective consumer software labeling program needs to address both types of threats. However, almost all certification programs focus almost entirely on common threats. Why is this the case? It’s because those threats can be addressed by assessing against a single common set of requirements. It’s relatively easy to develop a single questionnaire to assess all of these requirements.

What about the specific threats? How can they be identified beforehand, since they will be specific to what the software does and the environment it runs in? Is it possible to design a questionnaire that would address every threat that might apply to any consumer software product, deployed anywhere? And even if it were possible, wouldn’t that questionnaire be so long that nobody would fill it out?

There’s one labeling program that has addressed exactly these questions. In 2019, the Finnish National Cyber Security Centre (NCSC) introduced an IoT cybersecurity labeling program that assesses devices and their software, on both general and specific cybersecurity threats. The program includes five steps:

1. The manufacturer certifies their state of compliance with 18 basic requirements that form a subset of the ETSI 303 645 standard (the manufacturer must be in compliance with all 18 basic requirements before the label is awarded to them).
2. A third party “testing body” develops a threat model and risk analysis for the device and its software. This produces a list of cybersecurity threats that are applicable to the device and its software, and that pose a significant risk based on the intended use.
3. The testing body submits the threat model and a testing plan to Traficom, the Finnish Transport and Communications Agency. Traficom can suggest changes if needed.
4. The device and software are tested against all of the threats identified in the threat model, and the results are submitted to Traficom.
5. Based on the testing results, Traficom decides whether to award the label.

The most important feature of this program is threat modeling/risk analysis. If done properly, this can identify the main threats that apply to the software, given how it is deployed and used. Clearly, the competence of the "testing bodies", as well as of the organization(s) that grant the labels (Traficom, in this case), is crucial to the success of the program.

According to Traficom, this program has been well-received by IoT manufacturers as well as consumers. But the scale of this program is a tiny fraction of the scale of an eventual US software labeling program. Moreover, the Finnish program relies on a lot of "hands-on" involvement by Traficom, which won't be possible in the US. Is there a more scalable US program that could provide a governance model for a consumer software labeling program in the US?

We believe that the EPA's ENERGY STAR program points to a scalable governance model for the labeling program just described, with some changes. These are the features of EnergyStar that are most relevant for consideration for the consumer software labeling program:

1. There are two main types of organizations involved in this program: a) a laboratory tests products according to the test methods referenced in ENERGY STAR specifications; and b) a certification body (CB) certifies the product as ENERGY STAR approved.
2. While EPA directly approves the certification bodies, the laboratories are accredited by an accreditation body (AB). The AB accredits the lab based on their compliance with ISO/IEC 17025, which provides requirements for the competence of testing and calibration laboratories. Like the CBs, the ABs are approved by the EPA.
3. The criteria for approval of a particular type of product (such as a clothes washer) for ENERGY STAR certification, as well as terms for participation in the program, are clearly spelled out in a document specific to the type of product.

Red Alert Labs feels that all of the above features are worthy of consideration as the governance model for the consumer software labeling program. This means that, in the five steps for the program listed earlier, the laboratory will be the "testing body". Also, instead of a government agency approving the label, the Certification Body will approve the label.

There is one conflict between the device labeling program based on the Finnish model and the ENERGY STAR governance model: Because software security is a risk management challenge while energy efficiency is an engineering challenge, there are no physical quantities that can be measured to determine the level of security of a software product, as there are for energy efficiency.

However, it is certainly possible to describe, in general terms, the cyber threats applicable to particular categories of consumer software – e.g. communications software or real-time operating systems in consumer devices. These threats could be described in documents specific to each category of consumer software. For example, when a laboratory is developing a threat model for a consumer communications software product, they could start with the set of communications threats identified by a government agency like NIST. They could then narrow these down by creating a security profile (and perhaps adding new threats) for the software product in question. This will speed up the threat modeling process, plus it will make threat models for particular software categories much more comparable one to another, than if no guidance is provided at all.