Considerations for Developing a Profile of NIST's *Baseline for Consumer IoT Products (NIST IR 8425)* for Consumer Routers

On July 18th, 2023, the White House announced the next steps for the *Cybersecurity Labeling Program for Smart Devices to Protect American Consumers,* referred to as the "U.S. Cyber Trust Mark." In addition to announcing participation by the Federal Communications Commission and Departments of Energy and State, the White House also directed NIST to "immediately undertake an effort to define cybersecurity requirements for consumer-grade routers—a higher-risk type of product that, if compromised, can be used to eavesdrop, steal passwords, and attack other devices and high value networks." Towards this effort, this discussion essay will present NIST's initial thoughts and questions for the community related to consumer-grade router cybersecurity.

NIST proposes to use the *Profile of the IoT Core Baseline for Consumer IoT Products*, NIST IR 8425 (Consumer IoT Product Profile) as the starting point for developing requirements for consumer-grade routers since the assumptions and insights used to build the Consumer IoT Product Profile apply to this effort as well. For example, the primary use case of these routers is use in the home by household members and their guests, as assumed for a general consumer IoT product as part of creating the Consumer IoT Product Profile. Additionally, the cybersecurity outcomes of NIST IR 8425 were designed to be flexible in their application to different product types, allowing us to approach this effort by interpreting these outcomes for consumer-grade routers.

Scope

The White House announcement calls for NIST to develop requirements for "consumer-grade routers". "Routers" are network devices that forward data packets, most commonly IP packets, between networked systems. They may be wired (e.g., Ethernet), wireless (e.g., Wi-Fi), or both. "Consumer-grade" identifies those routers that may appear in an individual's residence such that their primary use case is residential rather than enterprise, industrial, etc. However, some small businesses may choose to use consumer grade equipment given the limited performance needs of those businesses. The presumption for consumer equipment, or small businesses that use consumer grade equipment, is that the manufacturer cannot assume the user has cybersecurity expertise or an ability to take significant action to secure the product.

Consumer-grade routers may be acquired by households in at least two ways:

1. Purchase of the equipment directly from a retailer
2. Bundling and/or renting of the equipment from a service provider

Each of these vectors have implications for how the cybersecurity outcomes of NIST IR 8425 could be met by the IoT product. Consumer-owned equipment may be fully managed by the household or may have some security services provided externally. Alternatively, whereas bundled/rented equipment will likely be managed in part by the service provider. Additionally, these variations and use cases potentially have significantly different features and capabilities to consider as part of the product, and thus may have different risk profiles and cybersecurity outcomes. For example, bundled/rented equipment commonly includes ISP gateway/modem capabilities in addition to home routing capabilities, whereas

retail purchased consumer-grade routers usually do not include these additional capabilities. **NIST seeks feedback on the appropriate scope for this effort and if there are other definitions of consumer-grade routers used by the community that NIST should consider.**

Consumer-Grade Router Product Components

Another aspect of scope relative to the Consumer IoT Product Profile is that the profile includes product components other than the IoT device. For a router product, this could include, for example, cloud services and/or a mobile app or other components. NIST IR 8425 defines the relationship of products to components as follows:

> "All IoT products contain at least one IoT device and may contain only this product component. In many cases, the IoT product may be purchased as one piece of equipment (i.e., the IoT device) but still requires other components to operate, such as a backend (e.g., cloud server) or companion user application on a personal computer or smartphone. Complex IoT products may contain multiple physical IoT devices, contain other kinds of equipment, or connect to multiple backends or companion applications as components.
>
> Though there are possibly a large number of component combinations that may create an IoT product, it is helpful to think of three specific kinds of IoT product components (other than the IoT device itself, which is always present in an IoT product):
>
> - Specialty networking/gateway hardware (e.g., a hub within the system where the IoT device is used).
> - Companion application software (e.g., a mobile app for communicating with the IoT device).
> - Backends (e.g., a cloud service, or multiple services, that may store and/or process data from the IoT device)."

In this context, the consumer-grade router equipment would be equivalent to the IoT device. Companion application software, specifically mobile and web-apps are common additional product components for consumer-grade routers. Backends are also a possible product component in this context. **NIST seeks feedback about the typical components of a router product that should be considered for this effort.**

Proposed Profile Presentation

NIST is also exploring how a consumer-grade router profile is best presented. As the announcement from the White House states, these new requirements will "permit the [Federal Communications] Commission to consider use of these requirements to expand the labeling program to cover consumer grade routers." A profile for consumer-grade routers could incorporate a similar approach as the Consumer IoT Product Profile and present requirements as high-level outcomes. High level outcomes define what is needed giving maximum flexibility for meeting that outcome. NIST proposes to create a profile for consumer-grade routers that would use the high level cybersecurity outcomes of the Consumer IoT Product Profile in NIST IR 8425 as a basis, while narrowing the potential requirements where appropriate. **NIST seeks feedback on the level of detail that is appropriate for the consumer-grade router profile requirements.**

Example Applicable Sources

NIST looks to available standards and guidance available for consumer-grade routers as starting points to tailor the recommended outcomes. For example, NIST has initially identified four standards and sets of recommendations in this space:

1. Broadband Forum TR-124 Issue 8 – Functional Requirements for Broadband Residential Gateway Devices [BBF]
2. CableLabs Security Gateway Device Security Best Common Practices [CableLabs]
3. BSI TR-03148: Secure Broadband Router - Requirements for secure Broadband Routers [BSI]
4. Infocomm Media Development Authority (IMDA) Technical Specification Security Requirements for Residential Gateways [IMDA]

These resources have helped us understand the landscape and approaches to consumer-grade router cybersecurity that exist today. Though the list above primarily identifies standards, other sources are also valid inputs for this effort. Other example resources that may provide information about consumer-grade router cybersecurity are:

- Cybersecurity documentation of an applicable technology (e.g., SP 1800-36, Trusted IoT Onboarding [SP 1800-36], IPv6 Cybersecurity [RFC6092])
- Consumer-targeted best practices such as those produced by governments [MASS][CISA][FTC][Defense], consumer advocates [CR], academia [UML][UBC], and other members of the community [IEEE][NCA][Router]

To continue this effort, NIST will analyze a variety of sources to effectively adapt our outcomes and develop requirements for consumer-grade routers. **NIST seeks feedback and recommendations from the community on applicable standards and other resources to inform the consumer-grade router profile.**

Proposed Source Analysis Process

NIST anticipates using a qualitative, community-involved approach to produce the consumer-grade router profile. As stated previously, the Consumer IoT Product Profile from NIST IR 8425 will serve as the starting point for this process. From there, NIST proposes analyzing identified standards and sources applicable to consumer-grade routers using the following process that will iteratively tailor the outcomes to be more applicable to consumer-grade routers:

1. Group the source document's requirements into their applicable Consumer IoT Product Profile outcome or sub-outcome.
    a. If a requirement does not have an applicable outcome or sub-outcome, determine if there is a need for a new outcome or sub-outcome to include the requirement.
2. Use the grouped requirements from steps 1 to tailor the outcomes of the Consumer IoT Product Profile outcomes if necessary, by adjusting or amending the language to more directly identify concepts reflected in the source document's requirements. The resulting outcomes can be considered an Interim Consumer-grade Router Profile.
3. Repeat steps 1 and 2 for each source, but rather than grouping the source document's requirements based on the Consumer IoT Product Profile, the requirements should be grouped

based on the Interim Consumer-grade Router Profile so that those outcomes are iteratively tailored based on each source document.

NIST will engage with the community throughout this process and gather regular feedback on the products of each step. Essays like this or other publications such as Online Informative Reference (OLIR) mappings can present NIST's progress to the community for feedback and discussion. Further, NIST can attend and organize workshops, roundtables, and other community gatherings to best facilitate participation and engagement in this process. Finally, NIST will remain open throughout the process to feedback and meetings with individual community participants asynchronously to any publication or event. **NIST seeks feedback on the proposed process and these community engagement plans and welcomes any suggestions from the community on how NIST can best enable their participation.**

Next Steps

NIST will follow an open and transparent process to develop the consumer-grade router profile. Community members are encouraged to contact NIST to discuss any of the concepts presented in this essay or other concepts related to consumer-grade routers, resources for cybersecurity in this field, the profiling the product cybersecurity criteria in NIST IR 8425, and other relevant topics. Feedback is to ensure our recommendations are an effective and meaningful set of requirements for consumer-grade routers. Please send feedback to iotsecurity@nist.gov and please watch our Program's Webpage for updates, events, and publications related to this effort.