High-risk String Classification Model

Background

Name Collision refers to the situation in which a resource name that is intended to be resolved in one naming system is inadvertently resolved in a different naming system, potentially leading to unexpected behavior such as communication being disrupted or redirected from its intended recipient.

Name Collisions may occur in information systems where different name resolution mechanisms are used sequentially or in parallel, without appropriate consideration of different potential failure modes.

When delegating new strings in the global DNS root, this may lead to new and unexpected behaviours with negative impacts for end users, businesses or other stakeholders. In a situation where name collisions occur, much of the responsibility to address an affected information system's shortcomings rests with the owner, provider or manufacturer of this system. However, if these negative impacts are likely to be severe, widespread and sustained, delegation of such a string should not take place until mitigating measures have been adequately implemented.

For these reasons, ICANN has implemented the Name Collision Risk Management Framework, following recommendations from the Name Collision Analysis Project Study Two Report, as directed by the ICANN Board on 7 September 2024.

The risk management framework described here incorporates risk acceptance thresholds. Previous work on name collisions did not address the topic of when to classify a string as being high-risk. Without a clear definition of what constitutes a high-risk string, name collision evaluations may be subjective, which can lead to uncertainty among applicants for new strings and inconsistent assessments between different evaluators.

This paper provides guiding principles to what thresholds are to be used when assessing a string for name collisions and when it should be classified as being a high-risk string, requiring mitigating measures before being delegated.

An Impact-based Model

A string should be classified as being high-risk if there is visible evidence that name collisions are likely[1] to occur with severe, widespread and sustained impacts to various stakeholders,

[1] The term “likely” in this context should be interpreted as something that can reasonably be expected to happen, corresponding to a subjective probability of at least 66%.

including the general public. The question that needs to be answered is what thresholds and criteria to use for this classification.

In designing a risk management framework it is common to use the potential negative impacts of an event to formulate the risk acceptance criteria. This approach is applicable to the name collision risk management framework as well.

Negative impacts as a result of name collisions could have unforeseeable consequences for a wide range of stakeholders in different sectors, countries and regions. It is impractical to identify all types of such outcomes or to provide any sort of algorithm for calculating the impact level.

Instead, different outcomes could be grouped into categories of stakeholders and then provide **guiding principles** in the determination of the risk level within each of these categories. For the name collision risk management framework, two distinct categories of guiding principles for the impact severity are provided. These two categories are **impact on public safety** and **impact on public confidence**. Modeling of different scenarios has shown that name collisions that have small impact on public confidence does not justify a string to be classified as high-risk, meaning that either few stakeholders are impacted or that many stakeholders may be affected but the impact level is low. Public confidence may therefore be used to gauge consequences on affected stakeholders as a collective ("the community").

However, the same modeling has shown the need to also define the public safety category. This category relates to potential impact on the well-being of people. It implies protection of the public from harm, including crime, disasters, and other threats. This category includes impacts affecting emergency services, such as police authorities, fire departments or other types of first responders. It also includes health care institutions and critical utility providers, such as water, energy and communication services. These are collectively called *Essential Entities*, and a list of such entities are provided in the next section.

For impact on public safety another set of criteria is defined. These criteria should be taken as examples of impacts that may affect public safety, not as an exhaustive list. These examples may have to be transposed onto other essential entities where impact may have an equivalent effect on public safety as the examples provided here.

1. **Impact on public safety**

    a. Emergency services may come under increased pressure to respond to an extent where response times are likely to be materially affected, causing tangible risk to public safety.

        i. Example: Emergency telephone services might experience availability issues due to widespread outages of underlying communication services.

        ii. Example: Fire alarm systems might experience stability issues causing them to trigger false positives, putting fire departments under increased pressure.

b. Environmental consequences may cause hazards to the well-being of people in affected areas.

    i. Example: A control system used in smaller hydroelectric power plants may fail, causing emergency water discharge that can be a hazard for people residing in the affected areas.

c. Essential entities supporting functions critical for public safety may be impacted to an extent and duration where the entity is unable to perform one or more of its primary functions, and where recovery can be expected to take at least weeks.

    i. Example: Internet Service Providers might experience severe and long-lasting stability issues, leading to wide-spread outages to an extent where public safety is impacted.

    ii. Example: Certificate Authorities might be impacted in a way which could lead to certificates being erroneously issued to the wrong entities, who could use them to commit fraud or to compromise the security of other systems.

    iii. Example: A cash register and logistics system in widespread use among supermarkets in a region is likely to fail, leading to an outage that could force about 1000 stores to close until the misconfigurations have been addressed.

2. **Impact on Public Confidence**

a. Loss of public confidence in the management and operation of the global DNS which is likely to be major, widespread and lasting.

    i. Example: Hundreds of thousands of home routers may fail and would have to be updated by manual out-of-band procedures, before regaining internet connection.

    ii. Example: A vast number of e-mail systems all around the globe may reroute internal e-mails externally if the string is delegated, potentially compromising sensitive information concerning an estimated hundreds of thousands of users, due to widespread internal use of the string.

    iii. Example: An applied-for string is in widespread use for internal purposes due to a vendor convention that was established decades ago. Delegation of the string would most likely be disruptive to a very large number of networks whose managers were following the vendor convention, as these configurations can not quickly be changed.

Essential Entities

The following list of essential entities roughly corresponds to those identified in the PDD 63 directive of the US government as well as those identified in the NIS2 directive of the European Union. This is not an exhaustive list, and entities with similar importance to public safety may be included in an assessment as deemed appropriate.

1. Utility providers
    a. Energy (Electricity, District heating and cooling, Oil, Gas, Hydrogen)
    b. Drinking water
    c. Waste water
    d. Waste management
2. Transport
    a. Air, Rail, Water, Road
    b. Postal and courier services
    c. Public transport
3. Financial
    a. Banking
    b. Payment service providers
4. Health
    a. Healthcare providers
    b. Laboratories
    c. Manufacturers of medical devices
5. Digital infrastructure
    a. Internet exchange points
    b. DNS resolver operators
    c. TLD name registries
    d. Trust service providers
    e. Providers of public electronic communications networks and services
    f. Cloud computing service providers
    g. Data centre service providers
    h. Content delivery network providers
6. Public administration
    a. Authorities supporting essential public functions
7. Food production and distribution
    a. Wholesale and industrial food production and processing
    b. Wholesale, distribution and retail of food
8. Manufacturing
    a. Production and distribution of chemicals
    b. Manufacturers of equipment critical for public safety, such as medical equipment, electrical components and machinery