Internationalized Domain Names Expedited Policy Development Process

Risk Assessment (E3)

IDN-EPDP Team Meeting #64 | 5 January 2023

Agenda

1. Roll Call and SOI Updates (2 mins)
2. Welcome and Chair Updates (5 min)
3. Continuation of Risk Assessment - String Similarity Review (80 mins)
    - Review risk model and apply against denial of service/no-connection and misconnection risks
    - Consider whether hybrid model is appropriate given level of agreed upon risk
4. AOB (3 mins)

Risk Assessment (cont.)

Why Risk Assessment?

- String Similarity Small Group recommended the hybrid model for the String Similarity Review
  - Hybrid model is designed to meet the **singular goal of risk mitigation of 1) denial of service and 2) misconnection**
  - Small Group **did not consider its implementation complexity**
- EPDP Team expressed **general support** for hybrid model, but some members expressed **reservations** about its implementation
- EPDP Team requested **ICANN org to provide operational input to help analyze the implementation complexity**
- ICANN org conducted an analysis to determine the potential number of comparisons that would need to be performed based on the models under EPDP Team consideration, i.e., levels 1-3 and hybrid model
  - Based on the 20 randomly selected gTLD strings, the **theoretical limit** for the comparisons **increases almost 38 folds from level 2 to hybrid model**
  - **Hybrid model may introduce more complexity**: as the String Similarity Review is a manual process, more people and more time will likely be required to complete the work
  - Costs for conducting the review will likely increase, and those **costs will be passed on to applicants**
- EPDP Team agreed to conduct a risk assessment of **1) denial of service** and **2) misconnection** to better **understand whether the hybrid model is commensurate with the risks**, and whether the risk levels are high enough to justify the added complexity and costs for applicants

Risk Assessment Overview

- **Purpose**: Assess the **inherent risk** level of the two failure modes involving domains, understand whether the mitigation measures are commensurate with the risks, and assess the **residual risk** level after factoring in the mitigation measures
  - **Inherent Risk**: The level of natural level of risk without doing anything to reduce the likelihood or mitigate the severity
  - **Residual Risk:** The amount of risk remaining after the inherent risks have been reduced by mitigation measures
- The specific risks being assessed are:
  - **Risk 1: Denial of Service / No-Connection**
  - **Risk 2: Misconnection**
- Assess the **Control Effectiveness**, which reflects the **effectiveness of mitigation measures**. The mitigation measures being considered include two options:
  - **Option 1: String Similarity Review Hybrid Model**
  - **Option 2: String Similarity Review Level 2 + String Confusion Objection Using the Hybrid Model**
- **Assumption**: mitigation measures mainly impact the **Likelihood**. As a result of either option, fewer strings may be delegated in the rootzone, lowering the likelihood of the two risks occurring
- Given the nature of these risks and for simplicity purposes, the risks are assessed from the perspective of **individual Internet end-users at the micro level**. Individual end-users' experience can be extrapolated to understand the collective experience by end-users at the macro level.
- ***Risk assessment is inherently subjective based on the professional judgement of the assessors***

How to Apply the Risk Assessment Model

01	**Describe the risks and consequences** of the risks occurring	• Risk 1: Denial of Service / No-Connection • Risk 2: Misconnection
02	Assess both the **Likelihood** and **Severity** of the risk occurring	• 2a. Likelihood rating can be assessed based on applicable examples inferred from the types of risks • 2b. Severity rating can be assessed based on applicable examples inferred from consequences
03	Assess the **Control Effectiveness** of mitigation measures	• Option 1: String Similarity Review Hybrid Model • Option 2: String Similarity Review Level 2 + String Confusion Objection using the Hybrid Model
04	Pinpoint the risk levels in the **Risk Rating Matrix**	• Inherent Risk = Likelihood x Severity • Residual Risk = Inherent Risk / Control Effectiveness

Step 1: Describe Risks and Consequences

	Risk 1: Denial of Service / No-Connection	Risk 2: Misconnection
Risk Description	A user attempts to visit http://example.X, reading it as being the same as the http://example.Y that, for example, he or she saw in an advertisement. After typing the address (http://example.X), the connection does not work as http://example.X is not registered.	A user attempts to visit http://example.X, reading it as being the same as the http://example.Y that, for example, he or she saw in an advertisement. After clicking on http://example.Y, the user arrives at a site controlled by a registrant different to http://example.X.
Consequences of Risk (examples)	• Cause user confusion and frustration • The user may conclude that "the Internet does not work" • A nuisance for users, like a typo, but no serious harm has arisen • Loss of confidence in the Internet	• May be more problematic than denial of service / no-connection and may result in the exploitation of user confusion • Arriving at the wrong site, even legitimate, can result in credential compromise and accidental exposure of information • If confusing similarity is maliciously leveraged, it can be a DNS abuse vector • When confusion is at the top-level, the possibility of DNS abuse is much greater than that at the second-level • Loss of confidence in the Internet • Distrust for the Internet

Step 2a: Assess Likelihood

Likelihood Rating		Description	Frequency (examples)	Scale (examples)
1	**Minimal**	Almost never occurs	A user almost never gets misled by domain names	Almost no user gets misled by domains names and incidences are rarely found anywhere
2	**Low**	Occur occasionally and in an isolated manner	A user gets misled by domain names only a couple of times and the incidences rarely repeat	Users in certain demographics get misled by domain names and the incidences are scattered
3	**Medium**	Occur several times and in a considerable manner	A user gets misled by domain names more than a few times and the incidences sometimes repeat	Users across several demographics get misled by domain names and many such incidents happen
4	**High**	Occur often and in an extensive manner	A user gets misled by domain names many times and the incidences often repeat	Users with diverse demographics get misled by domain names and the incidences happen in large scale
5	**Maximal**	Occur regularly and in a widespread manner	A user gets misled by domain names constantly and the incidences repeat regularly	Users all around the world get misled by domain names and the incidences are ubiquitous

What's the likelihood rating for:

- Denial of service / no-connection
- Misconnection

Step 2b: Assess Severity

Severity Rating		Description	Privacy (examples)	Financial (examples)
1	**Minimal**	A user may encounter negligible inconveniences	• Potential in revealing personal identifying information (PII) by getting clickbaited	• Potential in revealing banking / financial information
2	**Low**	A user may encounter few inconveniences, which may be overcome without any problem	• Email addresses and phone number leaked • Receive spam and phishing messages via email and phones	• Tricked to purchase fraudulent / unwanted goods or services
3	**Medium**	A user may encounter significant inconveniences, which may be overcome despite a few difficulties	• Online account credentials leaked (e.g., access to email, social media, etc.) • Reputational damage	• Debit / credit card fraud • Online shopping fraud • Denial of access to business services
4	**High**	A user may encounter significant consequences, which may be overcome albeit with serious difficulties	• Bank account theft • Biometric ID theft • Critical personal data / files theft	• Misappropriation of funds • Property damage • Loss of employment • False incrimination
5	**Maximal**	A user may encounter significant, or even irreversible, consequences, which may not be overcome	• Serious identity theft (e.g., social security number, impersonation using stolen passport / ID cards.)	• Bankruptcy • Life ruining debt • Loss of property

What's the severity rating for:

- Denial of service / no-connection
- Misconnection

Step 3: Assess Control Effectiveness

Control Effectiveness Rating		Description
1	**Minimal**	Effectively no mitigations in place
2	**Low**	Mitigation measure somewhat lowers the risk level but is barely effective
3	**Medium**	Mitigation measure is considered generally effective, but some risk remains
4	**High**	Mitigation measure is considered largely effective and small chance of control failure
5	**Maximal**	Mitigation measure is considered fully effective with a near negligible chance of control failure

What's the Control Effectiveness rating for:

- Option 1: String Similarity Review Hybrid Model
- Option 2: String Similarity Review Level 2 + String Confusion Objection using Hybrid Model

Step 4: Pinpoint Risk Level in Risk Rating Matrix

Severity	Likelihood 1	Likelihood 2	Likelihood 3	Likelihood 4	Likelihood 5
5	Medium / High	Medium / High	High	High	High
4	Low / Medium	Medium / High	Medium / High	High	High
3	Low / Medium	Low / Medium	Medium / High	Medium / High	High
2	Low	Low	Low / Medium	Low / Medium	Medium / High
1	Low	Low	Low	Low / Medium	Low / Medium

[i] Risk 1

[r] Risk 1

[i] Risk 2

[r] Risk 2

Likelihood

[i] Risk: Inherent Risk [r] Risk: Residual Risk